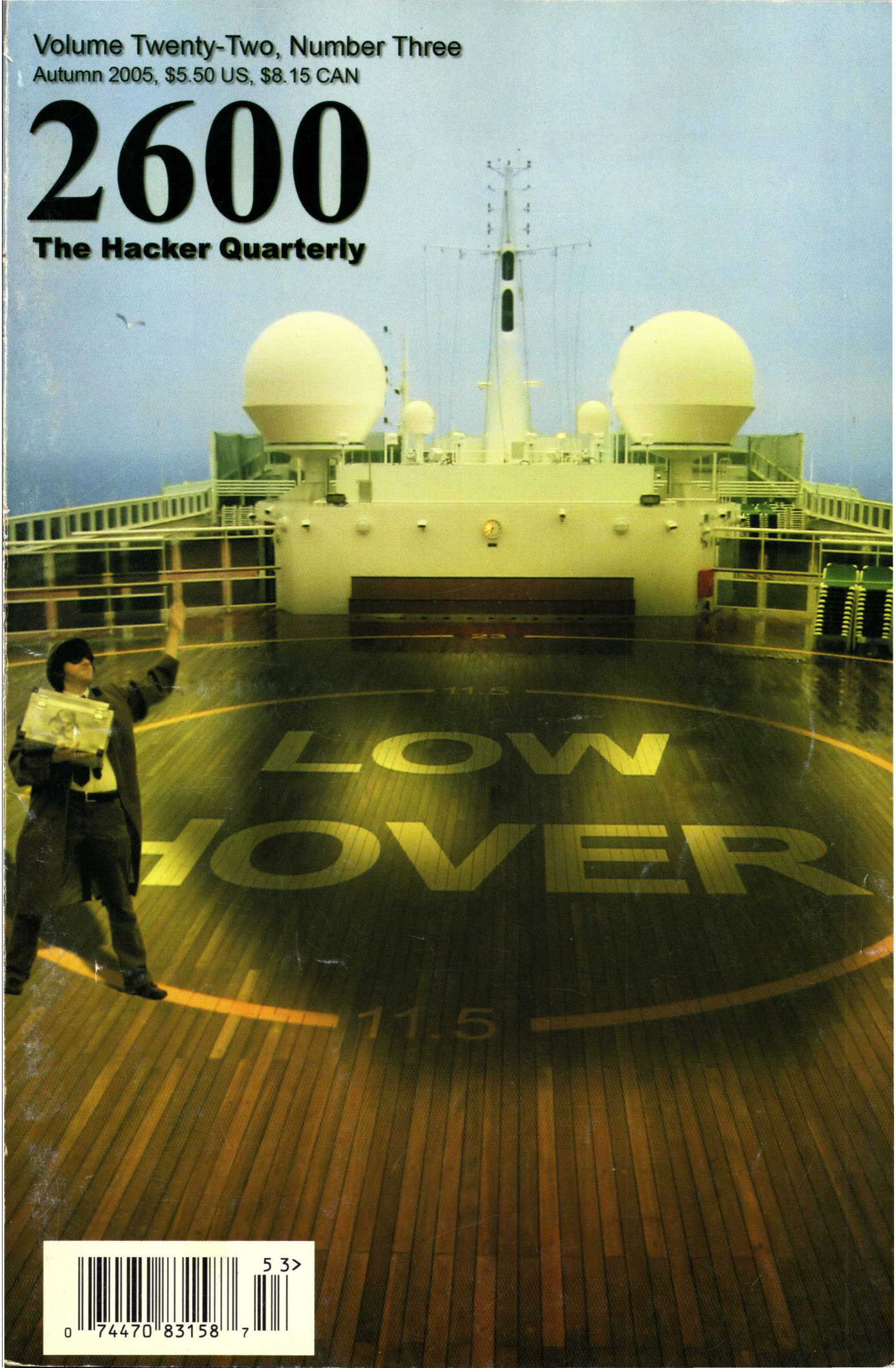
Volume Twenty-Two, Number Three
Autumn 2005, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7 53>

Mongolian Payphones

Yes, this is a payphone. In the streets of Ulaanbaatar, it's the human holding the phone who is referred to as the payphone.

Photo by Sasja Barentsen

The phone itself is a wireless CDMA phone. You give the "payphone" money and you make a call. And yes, most of them wear masks.

Photo by Hanneke Vermeulen

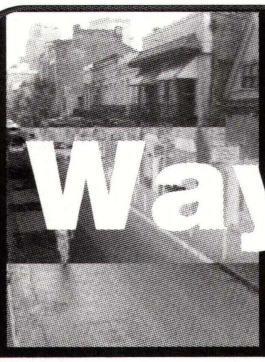
A more normal looking payphone but one that isn't seen in very many places. This one was found in the post office.

Photo by Sasja Barentsen

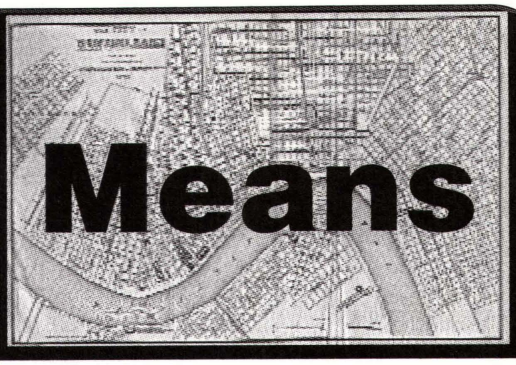
Here's a variation, designed to appeal to travelers and others who may have second thoughts about walking up to a masked person.

Photo by Sasja Barentsen

For more exciting foreign payphone photos, take a look at the inside back cover!



Ways and Means



Questions	4
Data Destruction, Covering Your Tracks, and MBSA	7
Stupid Webstat Tricks	9
A Randomizing Wifi MAC Address AP Hopper	11
Fun with the PRO-83	13
Getting More out of SSH	15
Using Tor and SSH Tunneling	17
Reverse Remote Access	19
Securing a Drive	21
Javascript Injection	22
Climbing the SonicWall	24
Verizon Fios - Fiber to the Home	25
Improving Stealth With Autoruns	26
SQL Exploits	27
Hexing the Registry	29
Letters	32
Not Working at a Call Center	46
Securing Your Wireless Network	47
The Continuing War on Spyware	48
Hacking Image Shack	49
I Am Not a Hacker	50
Security Pitfalls for Inexperienced Web Designers	51
A Peek Inside a Simple ATM Machine	52
How to Get Responses Through Deception	54
The Ancient Art of Tunneling, Rediscovered	55
Forging an Identity	57
Marketplace	58
Puzzle	60
Meetings	62

Questions

This is what it always comes down to. These are the things that are constantly getting us into so much trouble. And they're our best hope for significant change and true advancement.

Many of us become hackers for this very simple reason. We like to ask questions. We also don't readily accept non-answers or attempts to steer us away from discovery. Hence the resulting rebelliousness.

Computers, telephones, hardware of other sorts, and software of all types exist to be tinkered with, stretched to their limits, modified, taken apart, broken, and fixed. That's all part of the learning process. It's not enough to simply follow the rules that you have been given. You must understand *why* things are done in a particular way or else you're just mindlessly following commands without ever developing the capacity to come up with a better method. You might just as well be a machine.

If there's a theme that runs through the hacker community, it's that very desire to play around and experiment until you either understand the workings of a particular object of attention or have figured out a way to make it do something different than what you were originally told it was designed to do.

We don't think there's a single element of society that doesn't benefit from this hacker mentality. Thinking outside the box, trusting your instincts, keeping your eyes focused on the goal - those are common attributes in anyone who is actually pursuing something, not simply sitting behind a desk, in a factory, or in front of a television.

The hacking spirit can be found in journalism. It can be found in art. Or in investigative police work. Exploration of space. Even philosophy.

And the one thing nearly everyone in these categories can testify to is that most others on the outside view their efforts as a waste of time, overly idealistic, childishly naive, and sometimes even criminal. This is how it's gone over the centuries, from Galileo to Benjamin Franklin to Tesla. And we're all quite fortunate that their stubbornness and inability to listen to "common sense" won in the end.

Change does not come about from mindlessly following the rules. That's how dictatorships are maintained. Change is achieved through constant experimentation, the exchanging of ideas, and the freedom to do so. A society that views such things with suspicion is one that is doomed to stagnate and eventually fall.

These are elements that are found in the global stage all the way down to the parental level. It's all a part of the growing process, whether it's a child gradually turning into an adult or something much much bigger. In our case we see technology slowly evolving. And at the same time we also see our society grappling to deal with new things it's never had to deal with before. Email, surveillance, instant messaging, databases, biometrics... never before has so much changed so rapidly for so many. And that makes a lot of people nervous from the outset.

So it isn't too hard to figure out why questions would make them even more nervous. This is the common theme we've seen all throughout history and we see it especially strongly now, when there's so very much to question in the first

place. Those who ask questions are seen as troublemakers and even saboteurs. We see this brought up in every issue via our letters section. Those who don't follow the rules strictly and without question are punished and a message is sent to the others.

However that message is lost on the hacker community and for good reason. When someone is prevented from or punished for expanding their knowledge, all it takes is word of that to inspire more people to explore the exact same path and continue the work that was started. We like to think that over the years we've inspired a lot of people to continue with projects that might otherwise have been stopped in their tracks quite early on. That's the beauty of having a community. One or two may be stopped but it's next to impossible to stop us all. The only real danger lies in our becoming fragmented or forgetting the importance of continuing to question in these very basic ways.

Remember, there are two main reasons why someone views questions with hostility. If they don't know the answer in the first place, then questions can be an embarrassment as well as a risk of potential exposure. If they do know the answer but don't want it to be known by others, then it can be a far more sinister scenario. Whether by ignorance or by malice, the questioner is an inconvenience who must be silenced. This series of reactions to curiosity and investigation isn't going to go away anytime soon. And we're just going to have to get used to that.

The most important thing for us to do is not let ourselves be cowed by this reality. There are very few good things that have been created in this world that have come without risk. Knowledge certainly isn't one of them. And if we want to continue learning, we're going to have to be somewhat daring about it, especially in this day and age. That means experimenting with the hardware and software you've bought regardless of whether or not some government believes you have the right to. It means listening to whatever frequency you can access or decode with your own equipment. It means writing whatever words, theories, or programs you wish to make a point or to achieve a nondestructive effect. And above all, it means sharing this information with anyone else who's interested. Knowledge doesn't do the world a whole lot of good if it's kept secret, after all.

Naturally there are those who will use these methods simply to benefit themselves without much attention paid to the actual learning process. For instance, someone who has found out how to decode cable television signals and goes around selling decoder boxes is not the kind of person we're talking about here. Nor is the person who just mindlessly buys these things. Someone who figures out how to decode the signal or someone who is willing to learn how it's done from another individual is actually experimenting with technology and manipulating it in some way. Such a person is all the more likely to understand the theory behind it and could even be involved in designing a better system.

We've never condoned maliciousness or schemes that exist simply to get something for nothing. We believe most of our readers have little trouble seeing the difference between that and trying openly to defeat security systems and modify technology in various ways. The latter is absolutely essential for our development. Corporate lawyers, legislators, and, unfortunately, many teachers and parents see it all as part of the same thing. It's up to each of us to at least try and make the effort to explain the differences to them. And that's certainly not going to be easy, especially with the help of the mass media. But what we can't achieve as individuals we will accomplish as a community. There have been many victories over the years along with all of the discouraging news. We must figure out how to make each of these outcomes motivate us to keep doing what we do.

Any questions?

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2005. Annual subscription price $20.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, ST. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, ST. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, ST. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6 Extent and nature of circulation
7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
A Total Number of Copies	82,625	77,500
B Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4,663	4,642
2 Paid In-County Subscriptions	69	71
3 Sales Through Dealers and carries, street vendors, and counter sales	72,883	68,918
4 Other Classes Mailed Through the USPS	0	0
C Total Paid and/or Requested Circulation	77,615	73,631
D Free Distribution by Mail (samples, complimentary, and other free)		
1 Outside-County	444	445
2 In-County	3	3
3 Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	4,563	3421
F Total free distribution	5,010	3,869
G Total distribution	82,625	77,500
H Copies not distributed	0	0
I. Total	82,625	77,500
J Percent paid and/or requested circulation	94	95

"The good news is - and it's hard for some to see it now - that out of this chaos is going to come a fantastic Gulf Coast, like it was before. Out of the rubbles of Trent Lott's house - he's lost his entire house - there's going to be a fantastic house. And I'm looking forward to sitting on the porch." - George W. Bush, touring hurricane damage that at press time was estimated to have killed thousands of people, Sept. 2, 2005

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Dabu Ch'wald, Saldb

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

Broadcast Coordinators: **Juintz, lee, Kobold**

IRC Admins: **shardy, r0d3nt, carton, beave, sj, koz**

Inspirational Music: **Procol Harum, Cat Stevens, Roger Waters, 5678s**

Shout Outs: **Russell, Todd, Hanneke and Sasja, Gweeds, Bob and Margaret, ilya, the WTH Crew, Stuart, Adam, Jason**

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.
Copyright (c) 2005
2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752 Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

DATA DESTRUCTION, Covering Your Tracks, AND MBSA

by El Rey

First off, I would like to send a big shout out to LoungeTab for his article "Complete Scumware Removal" (22:1); his article was the inspiration for this one. Looking at the list of programs (many of which I have) I can see room to add at least two more, one free and one not so free but worth a purchase, in my opinion. Also, big thanks to Patrick Madigan ("Ad-Ware: The Art of Removal") (21:4), and shinohara ("Scumware, Spyware, Adware, Sneakware") (22:2).

Everyone knows that Internet surfing doesn't come without leaving behind a trail of history indexes, cookies, and whatnot. The problem is getting rid of it. SpyBot S&D and AdAware do a good job with this but I'd also like to recommend a program called Tracks Eraser Pro which is free to download (http://www.acesoft.net/download.➥htm). Not only does it do what SpyBot and AdAware can do but with free plug-ins it can erase histories and other digital "tracks" from popular software apps like PhotoShop, FrontPage, various Microsoft programs, and a long list of others. Not only that but there's room to customize what you wish to delete (which I'll give an example of down below). Even better than all of that is that this program permanently destroys data (not deleting it) by overwriting it with ones and zeros so no auto-recover programs can get back what you've deleted. It'll even clean the free space on your hard drive. By the way, all data is destroyed via DOD 5220.22-M.

Another program I've seen overlooked (in my opinion) is Microsoft's Baseline Security Analyzer (http://www.microsoft.com/technet/security/to➥ols/mbsahome.mspx - WinXP SP2 users will need to upgrade). Think of it as a Windows Update plus a poking and prodding of your security settings and seeing whether or not your system is secure. The problem I've found is that while you're running a scan the program will place several .XML files on your hard drive with your entire security specs plus your IP address to boot. With Tracks Eraser you can enable these files to be deleted - ahem, destroyed.

Delete vs. Destroy

Yes, there is a difference and it's basically what I said earlier: deleted data is marked by Windows to be returned to the free space, waiting to be overwritten. However it's still attainable by auto-recovery software (i.e., which is why we never sell our old HDDs on eBay). For example, after a long prOn movie we may decide it's better if we delete the incriminating evidence. With a quick drag-and-drop to the ol' Recycle Bin we assume it's nothing further to worry about... that is, until someone or something somehow manages to finagle their way to your box and run the right software and bingo! But this need not be your fate.

Once downloaded, run Tracks Eraser Pro and just click "Erase Now" and watch the messes get cleaned up. As for our prOn there's two ways of going about this: 1) delete it via Recycle Bin or whatever, and then open the program and find Eraser Settings->Windows->Clean Free Space and then click Erase Now. Depending on the size of your hard drive this can take a few minutes but since Secure Erasing is enabled by default (if not, then do: Options->Security->Secure Erasing) it'll be worth the wait. Second, Pro comes with its own File Shredder program from which you can drag-and-drop files there and destroy them. It's a rare occasion that I use the Recycle Bin for anything now. It even has its own cool little trash can icon on the desktop for you to use too - but open this app rather than drag something to it; it doesn't destroy if you drag directly to it. Once open, drag and drop to your heart's content. I'll have to email AceSoft about this.

Among your files you'll see your browser indexes, cookies, histories, AutoComplete's (what are you doing using IE?), and other assorted programs being thoroughly cleaned and destroyed leaving you with no tracks from which to be hunted down. I'm trying my best not to turn this article into a product review but I cannot really stress enough how fortunate I was to stumble onto this cool piece of software. The downside is that while it's free for a few days, you'll be nagged to cough up $29.95 for it but it was a

price I gladly paid. Once I'm done with my online banking or getting out of an SSL website, or just done browsing in general I always open this program up and watch it clean everything. There are tons of features in this program and I think it's best for the readers themselves to explore the full potential of this gem themselves.

MBSA

Another program I stumbled onto while browsing Microsoft was this program, the Baseline Security Analyzer. Open it, choose which computer (or computers, if on a network) to scan, and away you go. It'll automatically touch base with Microsoft Update and comb your system. Once done it'll spit out something akin to whether or not all your updates are installed on both Windows and Office, your MSXML Security Updates are installed, Windows Firewall is activated (mine isn't - though SP2's Security Center acknowledges my NIS 2003 is running smoothly), and various info on your services, file system, etc.

If you have a cable connection this all should take a couple of minutes and whatever MBSA says you're lacking, then it's all readily available to download off the links they provide. Here's the downside: MBSA leaves behind XML files on your hard drive that all start off with the following information:

```
*-* <../SecurityScans/WORKGROUP%20-%20
➥WORKHORSE%20%286-3-2005%208-20%20PM%29
➥.xml##> < SecScan ID="*0*" DisplayName
➥="*WORKGROUP\XXXXXXXXX*" Machine="*XXXX
➥XXXXX*" Date="*2005-06-03 **20:20:05*"
➥LDate="*6/3/2005** **8:20 PM*" Domain=
➥"*WORKGROUP*" IP="*XXX.XXX.X.XX*" Grade
➥="*5*" HotfixDataVersion="*2005.5.19.0*"
➥ MbsaToolVersion="*1.2.4013.0*" IsWork
➥group="*True*" SUSServer="" HFFlags=
➥"*4*" SecurityUpdatesScanDone="*True*">
*-* <../SecurityScans/WORKGROUP%20-%20
➥WORKHORSE%20%286-3-2005%208-20%20PM%29.
➥xml##> < <IPList>
<IP addr="*-XXXXXXXXXX*" />
< </IPList>
```

The Xs will be different for you depending on what label you've given your hard drive as well as what IP address you have. The purpose of this is so that MBSA can pull up past scans as a reference tool. However, since I get the funny feeling we will not need any past scans lingering around with this type of sensitive information, it is best we delete it. It's kind of ironic that a program written for security purposes has a very insecure way of storing data. Or should I come to expect this from Microsoft?

No need to fear, however.

Cleaning Up MBSA's Paper Trail With Tracks Eraser Pro

Remember, delete bad, destroy good. The location of these XML files is located in the C:\Documents and Settings\YOUR USER NAME\ ➥SecurityScans\ directory as well as within the C:\Documents and Settings\YOUR USER NAME\ ➥SecurityScans\Config\ directory.

Now, open Tracks Eraser and go to: Eraser Settings->Custom Item->Add File Folder And Item.

From here, click "Add" and watch the dizzying GUI that appears before your eyes. No need to fear for the force is strong with us.

All you'll need to know is that you must leave the wildcard option at its default. With that said click the Title box and give your new custom item a name, i.e., "MBSA Scans" and give it a description if you want. Next, find the scroll-down box that shows your HDD's files and folders. Find your Documents and Settings folder and double click on your user name, and then do the same for the SecurityScans folder. Now, find the Folder And Files That Will Be Erased box and click on "Add Folder" and watch your C:\Documents and Settings\YOUR USER NAME\SecurityScans*.* pop up in that box.

Now, for the other folder. Go back to the scroll-down box and double click the Config folder and then click "Add Folder" button again and watch the C:\Documents and Settings\YOUR USER NAME\SecurityScans\Config*.* pop up in the box underneath the previous one. Now, click Test at the bottom and you should see "Test Results: Test OK, X file(s) scanned." Now, click Save and exit out until you get back to the main GUI and hit "Erase Now." MBSA's paper trail is now erased forever.

Hopefully this was of some help to people looking for more security options. I've not even scratched the surface on what Tracks Eraser Pro can do such as writing your own plug-ins, and writing a custom item detailing registry items. Still, it's a cool little program. MBSA was a help to me too since when I first ran the program I saw I needed an XML parser update that Windows Update never showed me, and mind you, I thought I was running a very secure system (what with a router, software firewall, and various anti-crapware apps). MBSA's little XML presents were not appreciated, however, but with a little self-education I was able to overcome that problem as well.

To be fair there are other programs on the net that could possibly do the work Pro does for free but I'm of the philosophy that something good is worth paying for - and you pay for what you get. And to me a reliable track record of service is worth 30 bucks. Either way, it's up for the readers to decide and I hope that this article expands the knowledge pool of possible security options for those of us who need to feel safe.

Stupid Webstat Tricks

by stankdawg@stankdawg.com

Anyone who has ever maintained a website has probably used some webstats (short for Web Statistics) program to monitor their site's visitors. These packages all have various features, layouts, and designs but they all do basically the same thing which is to gather almost everything out of the log and save you the trouble of scanning through it yourself. Web statistics packages are plentiful and they serve a great purpose for the webmaster.

What is in a server log anyway? A web server log keeps track of all of the dates and times of every hit to every item on the site. Everything that is served up by the web server is logged including pages, style sheets, images, and anything else that is reachable over the web. The record of each hit contains several fields of information. This includes the agent (usually the web browser), the OS fingerprint, and the IP address of the requestor. Stats programs parse through your web server logs and collect and organize all of that dry, raw text data and put it into a nice, clean, human readable format. Some go above and beyond the basics to not only analyze the web logs (which contain IP addresses) but to see where they resolve. This allows you to see what sites are linking to you. They also may break down your hits by user-agent (usually a browser), country, OS version, and lots of other stuff that a webmaster can use to optimize their site. If your users all use a certain browser, you might put special code in your pages to give extra functionality to that particular browser for example.

But why would a hacker care about this? The answer is as simple as thinking of all of the things that are logged by the web server. Just having the raw logs alone could yield some great footprint information. You get the same benefits that the webmaster does! The thing to keep in mind here is that all hits are logged in a web server. The stats programs will gather them all up and far, far too many people make these stats publicly available.

Some webmasters actually want their stats exposed for some reason. They may think that it is some sort of service to their visitors or maybe a way to "show off" their hits. What they don't realize is that while showing off their hits, they are also giving a listing of almost every file on their server (or at least the ones that have been visited). The scary thing is that these visits include not only external visits, but internal visits as well!

You may be wondering what sort of things could possibly be found in someone's boring old stats pages. With internal visits being logged, some things appear that may not have been intended for public consumption. While the webmaster is working on or developing his/her pages, they are generating hits on those pages. I have gone to many "under construction" sites only to find that their web stats are working and I can see the complete list of URLS that they are working on! They certainly didn't mean for them to be public, but they are. I have entered contests early, joined sites that weren't open for business yet, and tagged guestbooks even when they weren't expecting any guests. Even if the site is not under construction, they are always working on some pages somewhere that are not publicly available yet and these links are picked up by the stats programs. Some companies use test servers for development and do not move anything to the live server. This is definitely the best practice to avoid having anything "accidentally" go public.

There are many statistics packages out there. I have tried many of them from the analog stats package to awstats and everything in between. We also have a few custom perl scripts written in-house to "watch the watchers" and see who is looking at what. For the rest of this discussion, let's focus on webalizer, which is the most common stats package that I see, as a base for the examples. It is no more or less vulnerable than any others, but it just gives a specific example for these scenarios.

By default, webalizer logs the top 20 pages visited. Webalizer can also be configured to provide a link to the entire list of URLs. The same holds true with the list of referrers. You may see pages that are listed that you didn't even know - or that you weren't meant to know - existed. Since you can see the exact pages that are being hit the most, you may find out that some quick redirection is happening and you may find a page that isn't meant to be traveled to directly. It may have source code in it that was supposed to be hidden or some configuration data in it that can explain how the site works. All of this would have been invisible to a user who didn't have access to public web stats.

One other thing to keep in mind is that when we say *all* pages, we really mean *all* pages. This means password protected pages and directories are also logged and therefore reflected on the stats page. You may not have the password to get into that directory, but you may be able to at least get the username. Another one of webalizer's defaults is to log the top ten users that login to a system account. If you want into that directory bad enough, it simply becomes a matter of brute force password cracking at this point.

Another interesting thing to keep in mind is the basic general espionage that can be done by looking at competitors' stats. It doesn't even have to be a competitor. It can be a friend, an enemy, or a random blogger on the Internet. You can see which of their pages are the most popular and use that information to your advantage. Perhaps you see that all of their hits are going to a certain web application or tool that they make available. You could write a similar application and try to steal their traffic away and over to your site, if you were so motivated.

You could also see where most of their hits are coming from. By default (and again, I am only using webalizer to have a consistent example and these techniques are just as effective with any stats package) webalizer logs the top 30 referrers in its stats generation. You can see where all of their hits are coming from and visit those pages to see why. Maybe they are advertising on a site that you hadn't heard of before which you could also be advertising on. Combined with the duplication of their page or application as mentioned earlier, you could not only copy them but also steal their own customers away from right under their nose.

Most people install webalizer into a directory named "/usage" which makes it easy to find on most servers. Other common places to find installations include "/webalizer", "/webstats", or just "/stats". You may also find it in a directory with the version number such as "/webalizer-2.01-10". If you don't have a particular target site or cannot find it on a particular site, then you can find many publicly accessible stats programs on Google by using some Google hacking techniques. If it wasn't googled, then maybe it is excluded by the robots.txt file (as mentioned in my article in the winter 2003-2004 issue of *2600).*

Here is an example of Google hacking for open stats packages. To find a site using webalizer, try these exact strings: "Monthly Statistics for" and 'inurl:"usage"'. This combines a literal string from the page and a static part of the string used in the URL. This URL string is a literal in the code and will not change unless someone has modified the code. Modifying your code is a practice that I highly encourage and changing a literal value is *very* easily done. It will protect you from the default hunters of the world by taking away publicly known literal strings from their search attempts. Use the same technique and apply it to your stats package of choice.

All of these vulnerabilities are easily fixed. One way to limit the potential for abuse is to read up on the package that you are using and how to configure it in such a way as to not show certain hits or certain pages that you do not want known. You can configure it to not show hits from the localhost or have it ignore hits to certain directories, for example. This method, however, is probably not the best approach. You may be working remotely and not from the localhost. There are always new pages or changes in your naming conventions that may allow information to slip through and you will be constantly plugging holes in your stats software. If you must make your stats public, at least make it a part of your security policy to regularly check these stats for sensitive data and update it accordingly.

There is one big and easy fix. If you are running a machine with some sort of control panel software, then your stats are usually only viewable by logging into the control panel (but not necessarily). If you are running your own server, or are installing your own stat packages outside of the control panel, then you really need to password protect the directory in which the stats are generated. It is very simple to add a password and now you have a reason to do exactly that. I do this, and so should you. Protect your stats packages with a password!

"The Revolution Will Be Digitized!"

Linkz: http://freshmeat.net/browse/245/ which has webalizer, awstats, and many more. Shoutz: The DDP, Doug, tehbizz, the listeners of DDP hack radio.

A Randomizing Wifi MAC Address AP Hopper

by Eprom Jones

In response to RSG's article in 22:1 concerning the "hunting" of wifi leeches, I offer this simple method of masking your MAC using Perl and Linux. My example focuses on my own Slackware system, because that is what I have, but should work on nearly all *nix and probably BSDs and OSX. That means *your* laptop (very sorry, Microsoft).

The first identifiable trait of a computer on a network is its MAC address. You can tell the vendor and sometimes model by looking up the octets. If the vendor is vigilant in its record keeping, the MAC address is traceable to the person who purchased it. Some people might want to avoid that for whatever reason.

One reason is to see if you can do it. I have an Intel b/g 2200 card built into my laptop and in the interest of a sort of superficial plausible deniability, I looked up the MACs assigned to Intel at good 'ol http://coffer.com/mac_find/. Since they had a bunch, I copied nine of them - 00:aa:00, 00:a0:c9, 00:03:47, 00:02:b3, 00:0e:0c, 00:04:23, 00:12:f0, 00:13:02, and 00:11:11. (They all start with zeros.) So then all we need to create a plausible yet random MAC is a simple Perl script to randomly select one of those nine prefixes, then fill in the rest of the hex digits. Cake.

```
        $one = "00";
        @twos = ( "aa", "a0", "03", "02", "0e", "04", "12", "13", "11" );
        @threes = ( "00", "c9", "47", "b3", "0c", "23", "f0", "02", "11" );
        @news;
        for ($i=0; $i<6; $i++)
          {
            $temp = sprintf "%1x", rand(16);
            $news[$i] =$temp;
          }
        $real_combo = rand(9);
        $newMAC = sprintf ("%s:%s:%s:%s%s:%s%s:%s%s", $one, $twos[$real_combo],
➥$threes[$real_combo],
                           $news[0], $news[1], $news[2], $news[3], $news[4], $news[5] );
        print "$newMAC\n";
```

This script makes a string Real:Intel:MAC:RandomRandom:RandomRandom:RandomRandom. A nYCe RaNdOm MAC. In order to assign your new MAC to your wifi adapter you can just add

```
print `ifconfig eth0 hw ether $newMAC`;
```

to your script. The "eth0" is the name of my adapter. Yours could be eth3, wlan0, en0, fxp0, etc. The "hw ether" tells ifconfig that it's going to change a hardware address of type ether. Before setting the MAC, you need to have loaded your wifi card driver. In order to prevent your card from automatically yelling out its name like a toddler trying to make friends, you need to load the wireless driver in non-associative mode. For my card:

```
print `modprobe ipw2200 associate=0`;
```

For other chipsets, the command will be different. The non-associative setting is not necessary. It just feels cleaner to know your real MAC was never broadcast at all.

So, putting these things together, here is a perl script AP hopper that gets you online with a random MAC:

```
#!/usr/bin/perl
#
# an ap hopper using random MAC by eprom.jones@gmail.com
#

use Term::ANSIColor qw(:constants);
use HotKey;

sub doit
    {
     print GREEN, "\n Doin it... \n", RESET;
     print `iwconfig eth0 ap $mac[$use]`;
     print `iwconfig eth0 essid $essid[$use]`;
     print `iwconfig eth0 channel $chan[$use]`;
     sleep (1);
     system (`/sbin/dhcpcd -d -t 10 eth0`);
     print GREEN, "OK...\n", RESET;
    }

sub stopradio
    {
```

```
     print RED, "\n quitin' time. \n", RESET;
     system (`/sbin/dhcpcd -k`);
     system (`modprobe -r ipw2200`);
    }

sub startradio
    {
     system (`modprobe ipw2200 mode=0 channel=0 associate=0`);
     print   `ifconfig eth0 hw ether $newMAC`;
    }

$one = "00";
@twos = ( "aa", "a0", "03", "02", "0e", "04", "12", "13", "11" );
@threes = ( "00", "c9", "47", "b3", "0c", "23", "f0", "02", "11" );
@news;
for ($i=0; $i<6; $i++)
  {
    $temp = sprintf "%1x", rand(16);
    $news[$i] =$temp;
  }
$real_combo = rand(9);
$newMAC = sprintf ("%s:%s:%s:%s%s:%s%s:%s%s", $one, $twos[$real_combo], $threes
➥[$real_combo],
                        $news[0], $news[1], $news[2], $news[3], $news[4], $news[5] );
print "$newMAC\n";

startradio;
system (`iwlist eth0 scan 1>/tmp/froglog.pad 2>/dev/null`);
open(INFILE,  "/tmp/froglog.pad")   or die "Can't hear no damned ribbits.";
while (<INFILE>)
  {
    if (/$\d{2}/)
      {
        s/ //g;
        /^(.*s:)(.*)$/;
        push @mac,$2;
      }
    if (/ESSID/)
      {
        s/ //g;
        /^(.*\")(.*)\"$/;
        push @essid,$2;
      }
    if (/$802\.11.+?/)
      {
        /^(.*802\.11)(.+?)$/;
        push @freq, $2;
      }
    if (/^.*Channel/)
      {
        /^(.*:)(.+?)$/;
        push @chan, $2;
      }
    if (/^.*Encryption/)
      {
        /^(.*:)(.+?)$/;
        push @crypt, $2;
      }
    $i++;
  }
close INFILE;

for ($ARGV[0] =~ /stop/)
  {
    stopradio;
    end;
  }

for ($ARGV[0] =~ /start/)
  {
    startradio;
    print GREEN, "\n\t ]-]o   }={o   Pick a Number 1 thru ", $#mac+1,"   o}={  o[-[
➥\n", RESET;
    for ($c=0; $c le $#mac; $c++)
      {
        if ($crypt[$c] =~ /on/)
          {
            $1=$c+1;
            print "\n$1  ", RED, "$essid[$c]", RESET;
```

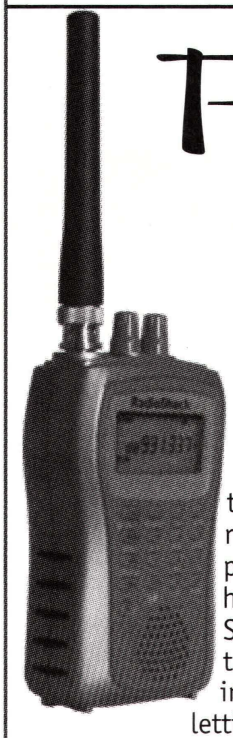
```
            next;
          }
        if ($freq[$c] !~ /g/)
          {
            $l=$c+1;
            print "\n$l  ", YELLOW, "$essid[$c]", RESET;
            next;
          }
        $l=$c+1;
        print "\n$l  ", GREEN, "$essid[$c]", RESET;
      }
    print "\n";

  $key = readkey();
  $use=$key-1;

  unless ($key !~ /[0-9+?]/ || $use>$#mac)
    {
      for ($#mac>0)
        {
          print GREEN, "\n You've chosen $essid[$use]", RESET;
          doit;
        }
      if ($#mac=0)
        {
          print RED, "\n\nSorry, bad scan. Please re-run.\n", RESET;
        }
    }

    if ($key !~ /[0-9+?]/ || $use>$#mac)
      {
        print RED, "hey \"visible\" NUMBERS only\n", RESET;
      }

    end;
}
```



Fun with the PRO-83

by Dit and Dah

Recently at a ham radio get-together at one of the local restaurants, our ham radio club president produced a small, silver handheld receiver from Radio Shack. He explained to us that this scanner was capable of locking into nearby frequencies and letting you know when someone was transmitting nearby to you, what frequency they were on, and what they were transmitting. He explained that he purchased this scanner, the PRO-83, for less than $60.

This was it, I thought, someone had finally put a frequency counter in a handheld scanner. I was expecting them to be far more expensive when they eventually came out, so I ran out and bought one. The $59.99 price was a one day thing, so mine cost me just under $100. I still consider that a fantastic deal.

PRO-83 Features

As was pointed out to the group of us at the restaurant, the PRO-83 could take two AA alkaline batteries or two AA NiMH batteries, which it can also charge. I find it to be very efficient in its battery usage; it can last at least two days of heavy usage on one charge (I haven't run it out yet).

The PRO-83 scans quickly (it scans the two meter amateur band in 5KHz steps in seven seconds), and can do frequency ranges (of which you can store ten in memory), channel scanning (200 channels in ten memory banks). And it of course has the ability to pick up nearby transmissions as soon as they start. In the PRO-83, this feature is called the "Signal Stalker."

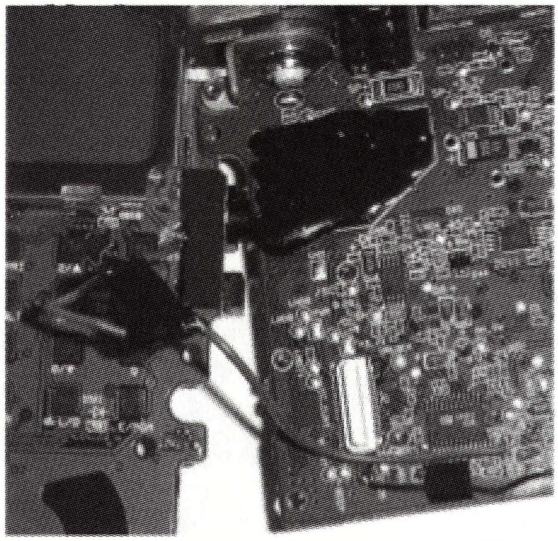
The PRO-83 packs a lot of features into a small keypad, so even if you're a coder like me, be pre-

pared to RTFM at least twice. The PRO-83 is a smaller sibling of the Uniden BC246T, which has alphanumeric channel tagging, trunking, and the ability to store found frequencies without user interaction in addition to the features of the PRO-83. In the BC246T, the "Signal Stalker" feature exists also, but is called "Close Call." The BC246T costs over $200, however, and since I'm poor and I don't feel comfortable modifying $200 pieces of equipment, I'll stick with the Radio Shack branded model.

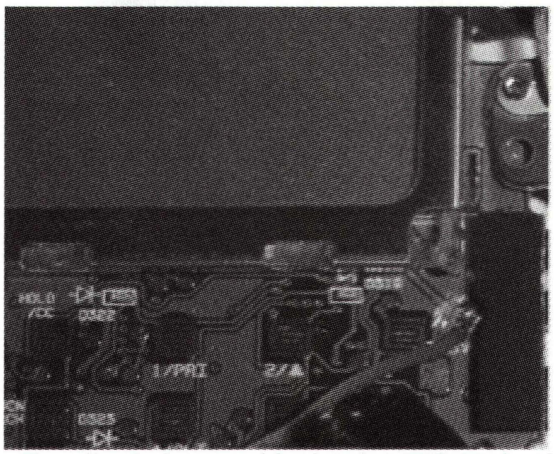
Undocumented PRO-83 Features

If you like taking full advantage of a scanner, you want to know all the mods available for it. There are some simple "keypad mods." The most useful one I've seen yet is holding down the HOLD, 3, and 0 keys while simultaneously turning on the power. This puts the scanner in a mode in which it operates much like a conventional frequency counter. You can use the arrow keys to scroll through to the band you want to be frequency counting on. [1] This in itself is amazing because most *stand-alone* frequency counters cost much more than $100. The Optoelectronics Scout, for example, costs $359.

Tapping the Discriminator



There's also a discriminator tap modification that was posted on the Internet by Gary Hahn, KB9UKD. [2] A discriminator is a circuit that voiceband filters the base-band audio coming out of the FM detector, so that the audio coming out of the speaker and headphone jack sounds good. If you feed a high-speed digital signal through a discriminator, it'll get distorted beyond the comprehension of the receiving computer. A discriminator tap, then, is a way to get audio out of the scanner before it goes through this filtering, enabling you to decode any data in it. For example, PL tones and 9600 baud packets can be extracted from your modded PRO-83 with the appropriate software. Much information can be extracted from ACARS airline transmissions and pager towers using the free PDW software (google it).



The discriminator chip in the PRO-83 is the TOKO TK10931V [3] and we'll be tapping baseband audio from its pin 12. This will bypass the voiceband filtering, the volume, and the squelch control.

The mod is very simple but involves disabling your PC/IF port. This is not that big of a deal given that the PC/IF port only enables you to program memory locations in the scanner from the computer. It's one way and cannot be used to control the scanner.

All that needs to be done to modify the PC/IF port of the PRO-83 to be a discriminator tap rather than a PC/IF port is to cut one trace on one board, and solder a capacitor from one point on the board to another point on the other board.

First you take out the six screws (two of which are in the battery compartment) necessary to open the case. The back part of the case has a connector for hooking the battery compartment to the other boards. You'll want to disconnect this.

The topmost board, the one with the volume and squelch controls on it, comes off with no effort, and is only connected to the boards below by a slot-type connector. To pull out the board under that, you'll need to remove six more screws. These six screws not only hold the back board to the case, but also hold the RFI shield to the board.

Having pulled out the back board, you can clearly see the trace going to the PC/IF port. It's right above the silk-screened label for the 3/SVC button on the back side of the back board. You'll want to cut this trace and solder a capacitor to the side of the cut still connected to the PC/IF port.

Gary says to use a 0.1uF ceramic disk cap, but after trying the 0.1uF cap, I replaced it with a 0.01uF metal film cap, and it seems to be working better. This was the recommendation of a piece of software I was using for data decoding.

Having soldered your capacitor to the board, you'll want to solder a wire to the other side of the cap and screw the back board, complete with its RFI screen, back into place.

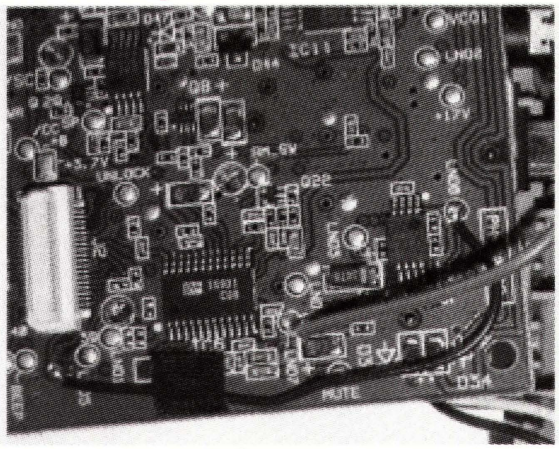
The other end of the wire goes to the tap point, which is labeled LND7 on the back of the topmost board, just to the right of the discrimina-

tor chip. This is the delicate bit, as the solder point is very small. Take your time here. Having made the contact, reconnect the topmost board, reconnect the battery compartment, and reassemble the unit. The mod is complete!

The first thing I did when I'd finished the mod was test it with headphones. The unit displayed "WirEd."

Oh no, I thought, it still thinks that port is the PC/IF port. Gary had warned of people experiencing this. I decided to hook the scanner up to the computer and give it a try anyway. I connected the PC/IF port to the MIC-IN jack on my laptop and tuned in a frequency on which data was being transmitted at 6400 baud. It started decoding data with no problems! So, the moral of the story is, plugging headphones into the PC/IF port after performing the mod won't necessarily tell you whether or not the mod was successful.

Also, I've found you can get the LCD to display "WirEd" if you connect a mono audio cable, so use a stereo cable to connect your discriminator tap to your sound card, even though there's only monaural audio coming out. Have fun!

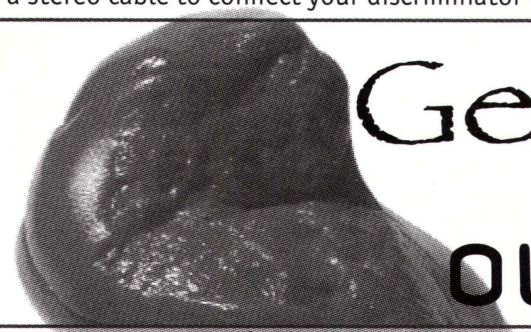


References

[1] http://groups.yahoo.com/group/PRO-83/

[2] http://kb9ukd.com/camera/2004/041126-➥Pro83/index.html

[3] http://www.tokoam.com/semiconductors/pdF➥/tk10931v.pdf



Getting More out of SSH

by Apratt

Everyone who sends private data over computer networks should learn how to take full advantage of SSH. SSH is not just a Telnet replacement, and you may be surprised just who is reading everything you type.

Five years ago in college, I was quite surprised to learn that an acquaintance on the third floor of my dorm was able to read AIM messages from me to someone off campus. I lived in the basement and he was separated from me by a few hundred feet of ethernet cable as well as a few Cisco 1900 switches. I didn't even think this guy was a computer enthusiast, but I suppose an ethernet sniffing program can make an enthusiast out of anybody. Luckily, we were on good terms and he showed me what he was doing. You can bet that most people who use ethernet sniffers *don't* let their victims know about it.

In this article, I will assume OpenSSH is the SSH package you use, but the information should apply to other SSH packages as well.

Most people just use SSH as an "encrypted Telnet." Even if this is the only way you want to use it, you should at least know about SSH's features that make it more convenient than Telnet.

You can execute commands on the remote computer without even really logging in. When using SSH from your command line, simply add the command you wish to remotely execute to the end of your SSH command. For example, where you would normally type:

```
ssh apratt@college.edu
```

type this instead:

```
ssh apratt@college.edu "ls public_html/*.jpg"
```

Hit enter, give SSH your password when prompted, and the task is done. If you use a private key file instead of a password (see below), there's even *less* you have to do.

Passwords used to be annoying to remember and type all the time, but not so with SSH. You can have SSH make you a private key file which acts as your password. If used properly, a private key file is more secure than a regular password due to its increased size and complexity.

(You may think that each character in your password equates to eight bits of a passkey. However, consider this: your password probably doesn't contain "high" ASCII characters (often represented by hearts, rectangles, foreign characters, etc.) or control characters (stuff like Escape, Tab, and Enter). This means that instead of each password byte containing 1 of 256 possible characters, it probably only contains 1 of 96 or so. Each character of a good password is really only

worth about 6.5 bits. The default length of a private key file is 1024 bits. Plus, using a computer-generated private key file prevents your users from selecting a password like "sex", "password", or their phone number.)

You can even encrypt your private key file with a passphrase for even *more* security. The Bad Guys would then need to possess both your private key file *and* the passphrase to decrypt it. Personally, I think that's overkill and just have a passphraseless private key file and a normal password to use when I can't use that. To have SSH make you a private and public keypair for use with the SSH2 protocol, use this command:

```
ssh-keygen -t dsa
```

If you prefer the RSA algorithm, just replace the "dsa" option with "rsa". If you want keys for use with SSH1, replace "dsa" with "rsa1". SSH1 and RSA each have some associated security problems and no real advantages over DSA, so you may as well stick with DSA-type keys and SSH2. ssh-keygen will ask you where you want your keys stored (the default is probably fine) and what passphrase to encrypt your new private key with. Abstaining from encrypting your private key with a passphrase will result in greater convenience, *but* you must make *darn* sure that *only you* can access that key. An unencrypted keyfile is just like a text file containing your password. It can be stolen by an ethernet sniffer if it is sent over a network by FTP, NFS, email, etc. (SSH doesn't actually send your key file during login, so that won't get it stolen.) Also be certain that its file permissions are configured to prohibit others from reading it. Anybody who Owns, confiscates, or steals your computer will be able to access every account that relies upon your key! The good news is that you can store your private key on something you can take with you, such as a mini-CD-RW, SanDisk, JumpDrive, MP3 player, USB wristwatch, whatever. Note that if SSH thinks your private key has the wrong file permissions, it will refuse to use it, and applying file permissions is tricky on many of those media. The server(s) you plan on connecting to with your new private key will need a copy of your new public key. Your public key file contains a really long line of nonsensical text and, as the name implies, you don't need to keep that text secret. If your destination server will only have one public key of yours, use FTP or whatever you prefer to copy your public key ("id_dsa.pub" by default) to .ssh/authorized_keys in your remote home folder on the destination server. If .ssh/autho➥rized_keys already exists there, just add your new line of text onto the end of the preexisting file on the next line. SSH should automatically look for your private keyfile (".ssh/id_dsa" in your local home folder by default) and use that instead of bothering you for a password from now on. If you store your private key somewhere else, such as on a mini-CD-RW use the "-i" option like so:

```
ssh -i /dev/cdrom/id_dsa apratt@college.edu
```

Making an appropriate symlink from your mini-CD-RW-based private key to .ssh/id_dsa will keep you from having to use the "-i" option needlessly.

One more thing about the mini-CD-RW with your private key on it: don't label it "MY SECRET KEY." Write "camping photos" on it or something boring like that. There's no need to attract unwanted attention from The Bad Guys.

scp is the SSH-ified version of cp (Unix's file copying command). To download a file, the command is:

scp college.edu:spring_break.mpg .

This example assumes the file you want is in your remote home folder. The lonely period at the end is just Unix's way of saying "Put the file in the folder I'm currently in." To upload a file, simply reverse the arguments (no lonely period needed this time):

```
scp spring_break.mpg college.edu:
```

You can even use a different username, specify a certain location, and rename the uploaded file at the same time:

```
scp spring_break.mpg
jsmith@college.edu:/home/apratt/public_h
➥tml/homework.mpg
```

Now that SSH doesn't ask you for a password, you can even make a script or cron-job to execute remote commands while you sleep. I like to schedule scp downloads and uploads for 3 am when bandwidth is plentiful.

Using sftp is like using other command-line FTP programs. GET, PUT, CHMOD, the main stuff's all in there. The main difference is that all communication is handled by a single SSH connection, as opposed to the unencrypted multi-connection silliness that is standard FTP.

It should be noted that everyone *should* protect their private key files with a passphrase to prevent them from being stolen. However, if you're not afraid of people stealing your persistent website login cookies or saved email password (both of which are usually sent unencrypted over the LAN/Internet), then leaving your SSH private key file "unpassphrased" isn't that big a deal. Depending on your paranoia level and SSH usage pattern, ssh-agent (included with OpenSSH) or Pageant (part of the PuTTY suite) may be a good compromise of convenience and security. These programs let you have encrypted keys, but cache your passphrase until you quit them.

Some Free SSH Clients

OpenSSH http://www.openssh.org/
MacSSH http://www.macssh.com/
PuTTY http://www.chiark.greenend.org.uk/~sg➥tatham/putty/

Using Tor and SSH Tunneling

by OSIN

One of the things about the sad state of affairs in the world today is that everything is being monitored. What used to be perfectly legal may bring the ire of a government down upon you. That was why I started to think about how to privately surf the web without someone trying to match log files with my machine's IP address. Of course, there are proxy servers out there, but still there are those damned log files that some sites keep for a long time. You never know. Some of you may be familiar with ssh tunneling and that is another way, but still you're counting on the one ssh server to forward your packets out to the web, or rather, to a proxy server. And how long are *those* log files kept? Unless you're the owner of the server, you should always assume the worst.

I've only been reading *2600* for about a year, so if I'm repeating information I apologize. But I know that there are some newbies like me out there who might be interested in this subject, so I thought it would be nice to revisit this subject with a twist. But I'll get to that later.

One way to privately surf the net (without buying proprietary software) is by using a program called Tor. Their own documentation states that "Tor provides a distributed network of servers ('onion routers'). Users bounce their TCP streams (web traffic, FTP, SSH, etc.) around the routers. This makes it hard for recipients, observers, and even the onion routers themselves to track the source of the stream."

You can download Tor at http://tor.free➥haven.net/dist/. If you're using a unix-like system, you should gunzip and untar the package you download in any directory you want. You will also need a package called libevent and it can be downloaded at http://www.monkey.org/~provos➥/libevent/. First, gunzip and untar the libevent package, then cd into the libevent directory. The installation instructions for Unix (I am using Linux) are very straightforward:

```
root@machinename# ./configure
root@machinename# make
root@machinename# make install
```

Then you must cd into the untarred Tor directory and repeat the above commands to build Tor. Check at Tor's website for more in depth installation instructions and documentation. At the time I wrote this article, the latest version of Tor was 0.1.0.10. However I had no problems during the build. For Windows users, the Tor website also has prebuilt executables that you can use on Windows based machines. I tried compiling Tor under Cygwin (a Unix simulation program) and it appeared to compile correctly on my XP box, but the program wouldn't run correctly. So I suggest you stick with the precompiled version.

At this point you're ready to run Tor. Assuming the executable is in your path, you should just be able to run the command "tor" in an xterm or shell. Tor recommends you *not* run it as root. The program should start up and begin to try to connect to the network. Running Tor in command line option allows you to see the messages it prints and a lot of times I've found this is good for debugging. Windows users should have a Tor icon on their desktop. Just double click it and it should run, assuming you chose a default installation.

One particular message you want to look out for is "Tor has successfully opened a circuit. Looks like it's working." That means you're good to go.

When I first started using Tor, I opened up Ethereal just to sniff my network and see where the packets were going. If you do the same, you'll see packets are going to several different IPs at various times. However, when I started up Tor I noticed the message "This is experimental software. Do not rely on it for strong anonymity." This concerned me, so I began to think of other ways to possibly add another layer of anonymity to the process. Could I possibly incorporate the usage of the well-known ssh tunneling with Tor? The answer is yes, you can.

In order to use this option, you should first

download a simple C program written by Shunichi Goto. You can find it at http://www.taiyo ➥.co.jp/~gotoh/ssh/connect.html. To compile, follow the instructions in the source code; they are very easy to follow.

One option that the ssh client allows you to do is to execute a command when you connect to an ssh server. This is very handy especially since the connect program can work with Tor. Therefore you can connect to an ssh server, but via the Tor network and not directly to the ssh server. Open up an Ethereal/tcpdump process to watch the packets flow before you connect to the ssh server of your choice and watch what happens.

First, let's start with a more simple example. Let's say you want to connect to an ssh server, but through the Tor system. Assuming Tor is still running and you have a valid account on an ssh server, you can connect with this command (all on one line):

```
/usr/bin/ssh -l [userid] [ip_of_ssh_serv
➥er] -o ProxyCommand="/tmp/connect -4 -S
➥127.0.0.1:9050 %h %p"
```

Note that I'm using the IP of the ssh server, not the DNS name. Try to stay away from any DNS name resolutions made from your machine to a DNS server. As an added measure, you might want to comment out any DNS servers listed in your /etc/resolv.conf file. However, keep in mind that some programs do their own DNS resolution calls. Anyway, in this example, I compiled the connect.c source code in /tmp, but you can do it anywhere you want. This method of connecting to an ssh server will be slower, but now you add a layer of anonymity that you might not have when directly connecting to an ssh server.

But what if you want to go a step further and surf the web through the ssh tunnel? Then you must run a more tricky command. You should go back and reread the man pages for the ssh client to refresh your memory on port forwarding, but I'll give you an example. Say you want to surf the web and use a tunnel to an ssh server on which you have an account. Now, not all ssh servers allow this maneuver, but let's assume yours will. First, you need an IP address and port number of a proxy server that will allow you to surf the web through it. Not all proxy servers allow this, but some do. You can find a list at http://www.pub ➥licproxyservers.com. But let's say you found one at 192.168.1.100 using port 8080. As a side note, don't use this IP in actual operation since it's a reserved internal IP address and I'm using it just as an example. Now, you must choose a port where you want your local machine to be listening for requests from your browser. Let's choose a random port, say 4567. This is the setup: when you make a request from your browser, the call goes to port 4567, then to port 9050 on your local machine, then through the Tor network to the ssh server which forwards the packets to 192.168.1.100:8080.

Before you can do this though, you must first change the proxy settings in your browser. Since browsers differ on where this setting is at, I won't be able to expound on this, but if you're a Mozilla/ThunderBird user, you can find it under Edit->Preferences->Advanced->Proxy. For Microsoft's IE (XP), the setting is located under Tools->Internet Options->Connections->LAN Set ➥tings. Choose the manual configuration and set the host to 127.0.0.1 and the port to 4567. Close out the first ssh session and open a new xterm session. Make sure Tor is running and you are connected to that network. Now you are set to run your ssh command (all on one line):

```
/usr/bin/ssh -l [userid] [ip_of_ssh_serv
➥er] -L4567:192.168.1.100:8080 -o Proxy
➥Command="/tmp/connect -4 -S 127.0.0.1
➥:9050 %h %p"
```

You should be prompted for your password for the ssh account. Do not exit out of this session. You need it open while browsing the web. Open the browser and start surfing. Watch the Tor xterm session and your ssh term session for any messages that might indicate that tunneling is not allowed or the proxy refuses to forward requests. If so, you may have to choose another proxy or your ssh server doesn't allow tunneling.

Assuming success, to test what IP address a website may be seeing you come from, you can go to a website such as http://checkip.dyndns.org. You should see the IP address of the proxy server, in this example 192.168.1.100. It's also a good idea to open an Ethereal/tcpdump process and watch where the packets are going. One thing I'm not sure of is where the DNS name resolution takes place if I have removed nameservers out of all my network files. Is it at the proxy? At the ssh server? Along the Tor network? Any experts out there may want to shed some light on this subject, but I didn't see any DNS requests in my Ethereal sessions coming from my machine when using the above method.

You should realize that browsing the web using the technique above will be slower, possibly very slow depending on what proxy server you choose, but vary the proxy settings to see how your response time changes. Occasionally I've gotten reasonable response times across the web using this technique.

Reverse Remote Access

by st4r_runner

Most businesses have some form of remote access for their employees. Well, what if your company doesn't want to support your linux/*bsd operating system? Or what if remote access is down and you can't connect to finish that important project? What do you do then? What if there were a way to have reverse remote access, or, in other words, have your company's network connect to you instead of the other way around?

There are several ways this can be done. This article will describe one way to do this. The basic outline of this scenario will go like this:
1) Send an email to your work address.
2) Your email client at your workstation at work will receive that email and launch a command.
3) Your workstation at work will then connect to your workstation at home.

Got it? Pretty simple concept. And just as easy to do to.

These instructions are based on the following assumptions:
1. At work you have a Windows OS workstation with Outlook installed.
2. At work you have the ability to connect to the Internet either directly or through an http proxy that supports the CONNECT method.
3. At home you have a linux workstation and a linux firewall (or some firewall that can do port forwarding).

The abstract would look something like this:

```
WorkXPworkstation --] CorporateFW/Proxy
➥--] [--Internet--] [--HomeLinuxFW [--
➥HomeLinuxWorkstation
```

Those are the pieces. To put them together we'll focus on one piece at a time.

//BEGIN configuration

WorkXPworkstation

Need:
1. Cygwin (http://sources.redhat.com/cygwin/setup.exe) base installation with openssh.
2. Outlook (or some MUA that can process rules and run commands). You must be able to keep your workstation powered on and logged in with Outlook running.
3. Corkscrew (http://www.agroman.net/corkscrew/) to proxy ssh through if you need to.

Config:
1. Outlook.
A. Create a client side rule that says "any email from myaddress@homeisp.net -] with subject of phone-home -] run command c:\ssh-home.bat".
B. Create c:\ssh-home.bat: (leave out the begin/end file markers when creating the files).

```
--begin file--
cd c:\cygwin\bin
cmd /k bash ~/run-ssh.sh
--end file--
```

2. Cygwin.
A. Create a ~/.ssh directory (if one does not exist already).

```
#] mkdir ~/.ssh
```

B. Create ~/.ssh/config file:

```
--begin file--
Host home
     HostName myhomefw.dyndns.org
     User myusername
     ProxyCommand /usr/local/bin/cork
➥screw proxy.work.com 8000 %h %p
     IdentityFile ~/.ssh/mykey
     RemoteForward 3389 localhost:3389
--end file--
```

C. Create a passwordless ssh key. The key must not have a password or this won't work.

```
#] cd ~/.ssh; ssh-keygen -f mykey -t dsa
```

(hit enter at the password prompts. this create mykey and mykey.pub)

D. Compile corkscrew in the cygwin environment.
E. Create ~/run-ssh.sh:

```
--begin file--
/usr/bin/ssh -N -F ~/.ssh/config -f home&
--end file--
```

HomeLinuxWorkstation

Need:
1. SSH server (I'd be surprised if it's not on your system already).
2. rdesktop client (http://www.rdesktop.org).

Config:

1. SSH.

A. Edit /etc/ssh/sshd_config (location will differ depending on distribution/installation).

```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
```

B. Copy the mykey.pub created earlier on your windows workstation into your authorized_keys file.

```
#] cat mykey.pub ]] ~/.ssh/authorized_keys
```

HomeLinuxFW

Config:

1. iptables port forwarding (replace xxx.xxx.xxx with your corporate public IP range and 10.0.0.2 with the IP address of your linux workstation).

```
#] iptables -t nat -I PREROUTING -p tcp
➥-s xxx.xxx.xxx.0/24 --dport 22 -j DNAT
➥--to 10.0.0.2:22
```

If you do not have a linux firewall then just create your own rule to forward port 22 into your internal machine. The beauty of the iptables rule on the linux firewall is that the firewall can still run its own ssh server while forwarding connections from your corporate network to your internal machine.

//END configuration

Now let's test some things out. From your WorkXPworkstation open up a cygwin bash shell and try running this command:

```
#] ssh home
```

If this is your first time connecting you will be prompted to accept the host key, so type "yes".

You should have been logged in without being prompted for a password. If not, then check the proxy settings.

Final Run

1. Send an email from your home email account to your work email account with a subject line of "phone-home".

2. Watch the output of "netstat -ltnp" to see when port 3389 opens up on your HomeLinux-Workstation. You can alternatively do:

```
#] while(true);do netstat -ltnp |grep
➥3389; sleep 5s; done
```

3. Once 3389 is listening on HomeLinuxWorkstation, you can run rdesktop to your WorkXP-workstation:

```
#] rdesktop -a 16 -g 1280x968 localhost &
```

Voila. You should now have an RDP connection to your WorkXPworkstation desktop.

Warnings

This is not the most secure setup. Yes, you will have an encrypted tunnel going to your corporate network. That's not the problem.

First, keep in mind that you have a password-less ssh key. If someone gets a hold of this key they can log into your machine without a password. Please do not try setting this up as the root user on your home machine. So do not put your mykey.pub into /root/.ssh/authorized_keys - that's bad.

Second, weakest link scenario: If your home firewall is insecure and someone was able to get in and steal your ssh host key and intercept your connections in a man-in-the-middle attack. If they didn't have your ssh host key, then a man-in-the-middle attack would be a little more difficult since the ssh client would fail complaining that the host key that it has stored is different. (Verify your ssh host key.)

Third, remember that your corporate policy may frown upon this type of outbound connection. Ask your manager/supervisor about it. You don't want to get fired over this. If you actually support your company's remote access environment then you can probably sell it as a way to get in to fix things when remote access is down (wink, wink).

In conclusion, this is a quick and easy way to get an encrypted tunnel into your corporate network for work you need to get done.

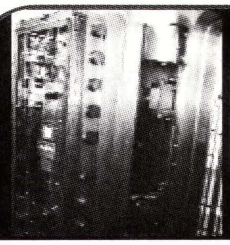
Shouts: imreut, King AdRock, frodo.

The VCDs from

The Fifth HOPE

are now available

They consist of all of the talks which took place in the two main tracks of the conference, which occurred in July 2004. There are 78 discs in total! We can't possibly fit all of the titles here but we can tell you that you can get them for $5 each or $200 for the lot. Much more info can be found on our website (www.2600.com) where you can also download all of the audio from the conference. If you want to buy any of the VCDs, you can send a check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or buy them online using your credit card at store.2600.com.



Securing a Drive

by Dr. Apocalypse
dr.apocalypse@gmail.com

Before I begin let me say that the following techniques only apply to Windows (sorry). What you need in order to follow the steps I'm about to describe: one external hard drive, one USB flash drive, a program called Sentry 2020 [1], Windows XP, and some common sense. First I'll outline the basic steps from a theoretical standpoint and then go into detail. There may be other programs out there like Sentry 2020, but this is the best one I've come across for this so far.

Basics

What we're going to do is create a virtual drive (called a data file by Sentry so I may interchange the two terms) on our external hard drive. All of our private information should be stored in this virtual drive. The data file will require an encryption key to decrypt all of the data stored in it before we can see it. Sentry provides us with ten encryption algorithms ranging from 56 bit all the way up to 1024 bit. The key will be password protected and we will choose to store it on our USB flash drive[2]. This will make it impossible to access the files on our external hard drive without inserting the USB drive. Obviously you do not want to leave this USB drive near your computer when you don't need to access these files. I suggest keeping it with you at all times (it's small so it can easily fit in your pocket), so that in the unfortunate event that authorities (or anyone for that matter) try to access your drive they will have no way of decrypting or reading the files on your external drive.

Specifics

Now we shall dive into the details of doing what I just described. First open Sentry and click the three dots next to the entry field labeled "Key File" to create your encryption key. Make sure you store this on the USB drive. Next, choose where your data file will go. Remember, this is the virtual drive that will hold all of your files so I'd recommend putting this on your external hard drive [3]. I think it would be wise to use maximum capacity on your external hard drive for the data file because someone may come up with a vulnerability for Sentry in the future that allows someone to gain access to the data file if they have access to the unencrypted space on the same drive. Plus, if you underestimate your storage needs and you need more space than you allowed yourself at some future point in time, you will have to resize the data file which erases everything in it at the time of the change. (Technically I think you have to delete the virtual drive and creating a new one with a bigger size.) Now it's time to choose your algorithm of choice and set your password. Use some common sense here: no easily guessable passwords! Choose your drive letter - nothing to really consider here as it's just a personal preference. And finally, set the timeout. I assume this means it will disconnect after a certain amount of minutes of inactivity, but I am unable to test this because I don't have any files large enough to take a an exorbitant amount of time transferring. Don't set this value too high because that would be a security risk. Don't make it read-only at first because Windows will need to format it the first time you mount it and it needs write access to do this. If you're really paranoid go ahead and make the data file read-only whenever you mount it as long as you don't need to put any new files in it.

Other Security Precautions

1. Make sure you don't have any viruses, keyloggers, or spyware on your computer because we wouldn't want anyone to know the password we chose.

2. One of the pitfalls of any encryption scheme is that in order to decrypt something your key or passphrase must be loaded into memory. To keep the feds from obtaining a RAM dump from your machine turn off automatic memory dumping and delete any dumps on your system. To do so: right click on My Computer } Properties } Advanced } Startup and Recovery Settings } Write debugging information and set it to "none." Delete %SystemRoot%\Memory.dmp to remove the last memory dump. Get rid of any memory dumps that occurred automatically upon receiving the infamous Blue Screen of Death by deleting the folder %SystemRoot%\Minidump [4].

3. As you should know, using the Recycle Bin does not get rid of files permanently! They can still be recovered. To remedy this I recommend wiping the free space on any of your hard drives (with multiple passes) weekly. Many free utilities exist that do this for you.

4. Delete your paging file (sometimes called a swap file) when you shut down your computer. To do so: click Start and select Run, type "regedit" (sans the quotes), and push enter. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl ➥Set\Control\Session Manager\Memory Man-

agement and change (Right click on it and select Modify) ClearPageFileAtShutdown to 1 (binary for true) [5].

Extension (for the really paranoid)

One technique for added security I thought of one day is creating a data file within a data file. This can be repeated several times [6]. Just make sure that when you create a virtual drive within another virtual drive that you make the second data file slightly smaller in size than the one it's created in [7]. For each data file use a different algorithm in order to slow anyone down that's trying to crack into your secret stash. More importantly, use a different password for each level in your hierarchy (i.e., primary, secondary, and tertiary data files). Make sure you dismount every virtual drive before closing Sentry! In my testing I was still able to access a file inside of a data file that was in another data file, which in turn was inside yet another data file after dismounting the highest level virtual drive and exiting Sentry.

Sources and Footnotes

[1] http://www.softwinter.com/ Free to try, $50 to purchase.

[2] I use a PQI Intelligent Stick 2.0 (512 MB, about $55).

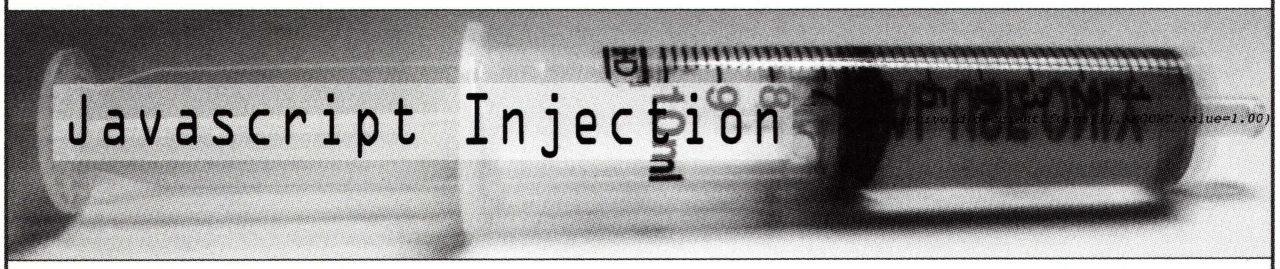
[3] If you don't have an external hard drive you may use the internal one in your computer, a zip drive, a floppy, or another USB drive; the only real requirement here is that your storage medium is large enough to hold whatever you want protected. The same goes for the USB drive: it may be replaced by a floppy, CD, or something similar, but both of those options are harder to safely and comfortably transport.

[4] *2600: The Hacker Quarterly* Volume 21, Number 3, Page 8-9.

[5] http://www.tweakxp.com/tweak31.aspx

[6] Note: Windows was unable to format a 2MB data file I created within a 5MB data file, which was in turn created inside of a 10MB file. I went with the default NTFS setting for the 5MB and 10MB virtual drives and didn't experience a problem; when I tried using NTFS for the 2MB volume I got an error, but Windows correctly formatted the 2MB data file using FAT.

[7] Note: Don't try to access the data file directly by clicking on its icon; use the shortcut to it that was created in My Computer for you.



by A5an0

You know, web hacking is a very different game than traditional "own-the-box" hacking. Instead of taking control of a target system, you usually try to exploit some flaw in the site's design to get information. Credit Card info, Social Security Numbers, breast sizes, they're all fair game once someone types them into a form. The most publicized attacks of late have frequently been SQL Injection (injecting SQL commands into a poorly written form that doesn't parse user input).

Well, the beautiful thing about information is that you can never have too much of it. While snacking on Oreos and Slashdot the other night, I stumbled across a little design flaw that can be easily exploited with good old fashioned javascript injection. That's right! We're hacking right from the URL. PHP and SQL squeezed all the Javascript out of your head? Come child (or kiddie, you make the call), let's dive right into the void.

The Discovery

Note: I will not be mentioning the *real* names of any involved parties, for their protection.

This story begins as any great one does: It was late and I had sugar. While surfing along the great flood of packets we all know and love, I stumbled upon the web page for a conference company. I'm sure you've seen them before. This is the kind of business that will put together a convention or conference, and then have you pay a registration fee either in advance or at the door. Well, this particular company was hosting some pretty cool sounding conferences coming up in a few months. So, a little curious, I drifted over to the "Registration" page. Scrolling down, I saw the "Early Registration" price. $20? $50? $100? Nope. $950. *Ouch!* The conference looked good but not $950 good. Being curious, bored, and a little hyper, I decided to keep looking around. Oddly enough, I found a little "Payment Services by VeriSign" banner across multiple pages. Hmm.... The cream filling was starting to work its way into my bloodstream, so I checked the source of the Registration page. I scrolled down and found a few interesting tags:

```
<FORM action=https://payments.verisign.com/payflowlink method=post target=_blank|<IN
➥PUT type=hidden value=jblow name=LOGIN| <INPUT type=hidden value=Verisign name=PART
➥NER| <INPUT type=hidden value=950.00 name=AMOUNT| <INPUT type=hidden value=S name=
➥TYPE|<INPUT type=hidden value=SecurTek.Conference name=DESCRIPTION| <INPUT type=sub
➥mit value="Early Registration"| </FORM|
Jackpot!
```

The Exploit

In case you have yet to realize it, my goal at this point wasn't to steal card numbers or email addresses. I just wanted to go to this conference. Looking at the above HTML, I saw one line that stood out most:

<INPUT type=hidden value=950.00 name=AMOUNT|

Hmm... it seems that the payment engine gets all the price and event information right from this page. Looks like this is gonna be a quickie.

It would be really cool if I could lower the price of this conference. The price is right in this tag. Logical conclusion: change the tag! Now any weenie with a dial up would tell you to download the source and change the tag, click the button, and poof! Guess again. Most of these pages have a small referrer built into them that will keep you from doing this. So, we're gonna hit it with style: javascript.

First things first: I need to figure out what number form this is on the page so I can change it. Easy enough: I whip open the source and just count the number of <form| tags I see before this one. (Note: the first <form| is number 0, not 1. Keep that in mind, or it will be *hell.)* OK, cool, this is form number 1 (actually the second one).

Next step: Make sure that I have the right form. To the address bar Batman! I bang out a quick

javascript:alert(document.forms[1].AMOUNT.value)

into the address bar in Firefox (IE users, no worries, this will work on Internet Exploder as well).

Now, let me break down what I just did.

```
                                    javascript:alert(document.forms[1].AMOUNT.value)
                                                  ^              ^         ^      ^
                                                  |              |         |      |
This tells the browser to alert me -------        |              |         |      |
This tells the browser which form I'm interested in-------|      |         |      |
This is the name in the INPUT tag ----------------------------|      |
This tells the browser I'm interested in the value of the form --|
```

When I press enter, this little snippet of code causes an alert box to pop up displaying 950.00. Sweet.

Forget the foreplay. It's time to hack. Now that I'm sure I'm dealing with the right info, I make my move. I just plug

javascript:void(document.forms[1].AMOUNT.value=1.00)

into the address bar and hit enter. (You can probably infer what all of this code does. The only real change that may not make sense is the "void". All you need to know is that "void" tells the JS to change something.) I Hit Enter and nothing happens. Cool... I hope.

So just to be safe, I drop our good friend

javascript:alert(document.forms[1].AMOUNT.value)

back in, and he just says 1.00.

The final step in our dirty little dance: Now that the value for AMOUNT has been changed from $950 to $1, I think I can finally afford that conference. Let's see if my sugar induced orgy of code was worth it. I click the button. And to my absolute joy, I see a page asking me to enter my credit card information, as well as name, address, etc. The sweet part is that this page is asking me to authorize a charge of $1 to my card for this event. Needless to say, if you have come up with a root dance over the years, this is when you do it.

Conclusion

I'm sure that anyone can find a practicality flaw in this particular application, but that's not the point. While getting a 99.89 percent discount is a sweet deal, what I hope you got out of this article is a basic understanding of a technique that, sadly, isn't so common anymore today. Don't get me wrong. I love SQL, PHP, and I get giddy every time I get my hands on a new 0day, but sometimes the easiest route is the simplest. I hope you learned something that you can use, or at least think about. Enjoy and keep learning! I need sleep. Have a nice day.

Climbing the SonicWall

by Kn1ghtlOrd
Kn1ghtlOrd@hotmail.com

Since 9-11 Internet and network security have moved into the foreground. The various companies that provide different security services have come up with the idea that there is a need for an all-inclusive network security appliance that includes anti-virus, anti-spyware, intrusion detection, content filtering, and firewall services. A few of the more popular companies to produce these products are Symantec, McAfee, Nortel, Watchguard, and Sonicwall. Although the configuration and administration of these devices vary, they all have the same basic principals behind them.

I will be talking specifically about the SonicWall security appliances but the basic principals could be translated unto the other devices as well. The SonicWall comes in a few different models. The TZ 170 is a small ten user box similar to a router with a five port switch built in while the Pro series consists of the 1260, 2040, 3060, 4060, and 5060. Most of these boxes are pretty similar. They are rack mountable units that have ports on the front for LAN, WAN, DMZ, and VPN. The higher numbered models also support 10/100/1000 communications. The 1260 has a 24 port switch built in as well. There are a few other models which I will not describe too much because they are the same as all the ones listed above, just with wireless capabilities built in. I will however mention the SonicPoint which is a wireless access point that is self configuring on a SonicWall system, which means once it is plugged into the network the main SonicWall is operating on, it will automatically be configured by the main firewall to mirror all of its settings.

The operating system that is used on each box is a proprietary system known as the SonicOS and there are two versions, standard and enhanced. With the enhanced version all the rules and settings are defined by using objects, so if you have a router or a wireless device attached that needs special rules you would define that router and its information like IP address, zone, authentication method, etc. into an object within the SonicWall system. So if there are changes to that device you only need to change it once in the SonicWall and it will affect all the rules set for that object. If you have any experience with modular or object oriented programming than you probably understand what I am talking about.

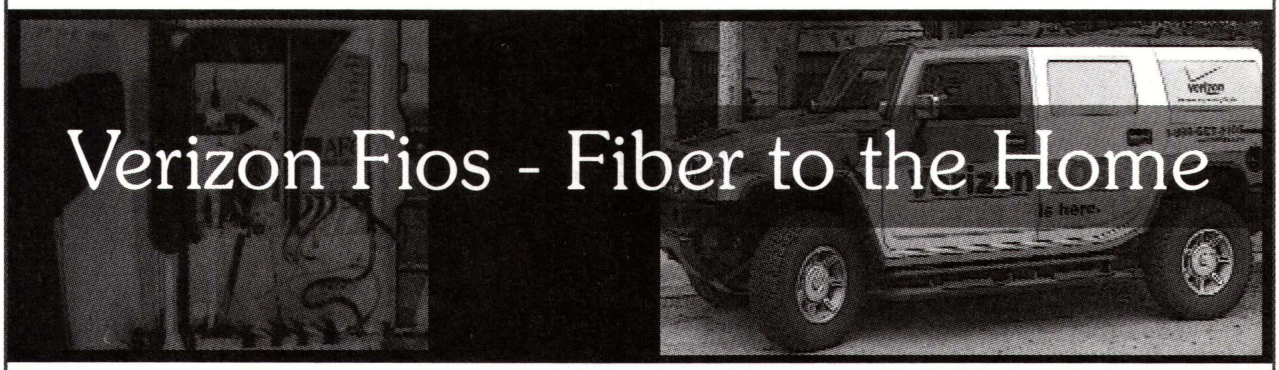
Another feature of the SonicOS Enhanced is that it has the ability to utilize an extra port that is included in all the Pro series models. The SonicOS Standard can only use the LAN, WAN, and DMZ/VPN ports. There is a fourth port that can be configured to another LAN or WAN port, so if you set it up to be a WAN port you can have two separate Internet connections and share the load or do a fail over service. The SonicWall Pro series appliances can easily run you around $3000 and this is without anything else. SonicWall also provides an intrusion prevention service, which is pretty robust, but it uses snort rules contributed by the open source community and they charge around $1500 a year for that service alone! Also, they have a content filtering service, two types of anti-virus for the box and one for individual nodes attached to the machine. They also have an anti-spyware solution and a logging service called Viewpoint, which takes the raw data that the SonicWall collects and summarizes it into nice little charts and tables for administrators to look at. The only thing I don't like about this is the viewpoint server can be a normal PC with at least 512 RAM and a 2.8 GHz processor running XP Pro, and the software installs a version of Tomcat web server and MSSQL server onto the machine. Now you may ask what the big deal is. But it is a very big deal. If the Viewpoint server were able to be compromised then you could log into the SonicWall as an admin *without* verification. On the main status page there is an area where you can log directly into the SonicWall, completely bypassing any security or knowledge of the IP address or the login methods. The Viewpoint server also supports concurrent login from the administrator.

Here is an example of how I broke into our own system during a pen test. Our system is composed of three remote offices and one corporate

office. Two of the remote offices connect through a secure digital line that directly connects the offices to the corporate offices. The third office is for a buildings and grounds crew and they have only one machine. The manager logs into our network by dialing into a Netgear dial-up router which patches it into our network, kind of like a VPN. So I sat at home and dialed into the network. I already knew the admin password but for the sake of a good pen test I ran Ethereal and sniffed out my manager accessing the viewpoint server which gave me the IP address of his machine and the server. I ran a nice little program that sniffs passwords out of a network based on IP address so I got the password to the Viewpoint server. I proceeded to connect to the Viewpoint server with the username and password I sniffed out and, like I said, the Viewpoint server supports concurrent login from the admin so I connected and proceeded to get to the main SonicWall device. The main box does not support concurrent login, but if there is already an admin on you can either boot him off or try again later. The Viewpoint server can help you monitor his activities. Once inside the SonicWall you have free reign to open ports and services, unblock content filtering, stop services, or even turn off the Internet completely. You could also set special rules within the virus scanner to allow your virus or whatever you want.

As you can see, this is a big hole in the system. When using the Viewpoint server to access the SonicWall it sends a request for a certificate from the main box to verify it, but the certificates are allowed to be different. In our situation the certificate is sent from the default IP address (192.168.168.168) but the actual IP address of the box is 192.1.1.99 so the certificate recognizes this and simply asks you if it's OK that they are different so you are able to login anyway. Another way I logged in was with the use of an unprotected wireless router still plugged into the network. With this, I performed the same tasks as mentioned above.

I hope this article has been beneficial. By the time it's published I will have a website up on Yahoo! Geocities that will have all the manuals for the system in PDF format for anyone to download. This information is *supposed*to be confidential, but what is the fun in that? I only have a few megs of storage on Geocities so I will include the most informative of the manuals, but I will also include a list of manuals that I have available and if you would like them just send me an email and I will send them to you.



by striker

On Long Island you have two choices for Internet access: the Dolan Dictated Optimum Online or Verizon DSL. Cable is faster, but ridiculously overpriced. Verizon is cheap, but uploads are slow. Now, there is a better choice.

Verizon has begun deploying in limited areas an entire residential fiber infrastructure. The offering now includes three bandwidth options: 5/2, 15/2, and 30/5. 5/2 costs the same as DSL, but has kicking upload speed. In less than year, Verizon will also begin offering TV service over the line - competing directly with satellite and cable.

My big question was simple. *Why??* Verizon was formed through traditional, old school phone companies. They got dragged into the DSL business kicking and screaming, forced by competition from the cable companies. After plenty of research the answer became clearer. The Telecommunication Act of 1996 forced all of the phone companies to play nice in the sandbox and share their copper. All kinds of competition opened up, allowing the average consumer to choose their own local and long distance companies, while forcing phone companies to foot the bill to maintain the infrastructure. Maintaining the tangled web of copper phone lines is very expensive. Most of the copper hanging today is old and noisy. It needs to be replaced. That's gonna cost a lot of money.

So how do you rid yourself of pesky competition and aging copper? One word: Fiber. Fiber optic cable has huge bandwidth capabilities and doesn't degrade. Newly installed fiber optics belong to Verizon and are not considered public or municipal lines. While it probably cost a fortune up front to roll out, in the long term fiber will require fewer maintenance runs. Lowering operat-

ing costs raises stock value. Sweeet.

Tech Talk

The technology is pretty straightforward. At the central office is a box called an optical line terminal. It acts like a gateway, taking feeds from the voice switches, Internet routers, and eventually TV signal head ends. All of these signals are WDM coupled and sent on their way via laser wavelengths: 1310nm for upstream voice and data, 1490nm for downstream voice and data, and 1550nm for downstream video. To be clear, the voice signal is *not* VOIP. The voice signal is modulated over the fiber.

From the CO, fiber feeder lines travel the poles to local Fiber Distribution Hubs (FDH) which can support up to 216 homes. From there the lines snake out to 12 port distribution terminals placed every few hundred feet that connect to the homes.

On the side of the residence is mounted the Optical Network Terminal (ONT). This box looks like a bigger version of the regular grey NID where copper terminates. The color is the only similarity. Inside the box is a plug where the fiber terminates. This connection is closed up and is only supposed to be accessed by Verizon. Also in the box are an RJ45 port and 4 RJ11 ports. The technician will run Cat5 from this box to your computer, and tie your existing home wiring into the RJ11 connectors. The technician will also mount inside your house an AC adapter and a UPS. Verizon claims that the UPS will provide five hours of operations. The AC adapter and UPS are wired back to the ONT to provide power and system status. Internet connectivity is still controlled via PPPOE. Verizon FIOS appears to use the 70.104.0.0/13 block.

The final action happens when the technician uses the copper line to dial up to the CO and switch the phone signal over to the fiber. He then cuts down the copper from the house to the pole. Bye bye competition.

One of the great cost savers for Verizon is that the fiber connections from the CO to the residence are all passive - no powered or active components. Nothing to burn out. The Verizon NOC can proactively monitor the health of the UPS and ONT.

The price is right, the speed is excellent, and service has been robust so far. Finally, having fiber optics terminating at your house is just darn geek-cool.

For more info straight from the horses mouth, see http://www.nefc.com/2004_Downloads/FTTP➥_NEFC_2004.zip

Improving Stealth With Autoruns

by BrothaReWT

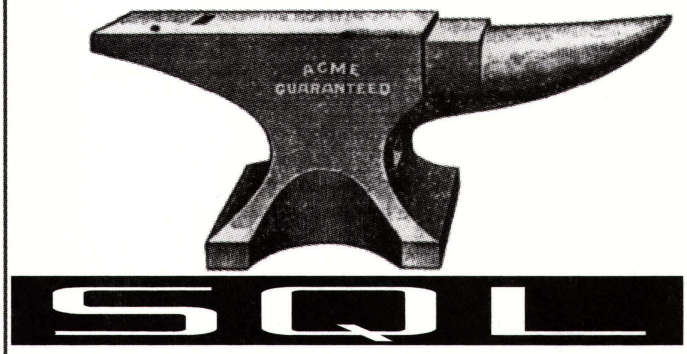
This article explores further what Forgotten247 wrote in 21:4. This article is intended to invoke thought and awareness, not cause damage or malicious activity. Anything you do with this information is your own fault.

I work day to day as a computer repair tech. In my normal day I work on five to eight Windows XP/2000 machines. One tool that I use every single day is "Autoruns" which is available at www.sysinternals.com. This tool will show you every single program that runs as soon as the computer boots. Compared to Autoruns, MSCONFIG is a child's toy. Autoruns has been an invaluable tool in the day to day battle with spyware and viruses. One of the great features of Autoruns is that it will show you all the DLLs that get loaded into Explorer.exe. This list will range from about 25 to 60 DLLs on some machines. But one thing you can count on is that Microsoft adds in a few that the average user will never notice if they are modified. A slick way to hide whatever tool you are trying to hide and keep running at every boot would be to rename then replace one of these DLLs with one that will point to your program or, hell, you could drop the payload from inside the DLL if you want. Some of the DLLs in the aforementioned list will even run in Safe Mode! An example of one of these DLLs would be %windir%\system32\Cabview.dll. This DLL will most likely not be missed or even noticed by the user. One thing to keep in mind is that Autoruns

will show the publisher of a DLL (for example, Microsoft or Grisoft for AVG Antivirus and Qualcomm for Eudora). So when you are coding the DLL to use for this, be sure to drop an official name in the publisher field. This idea came to me when I was removing a VX2 variant that used random DLL names and ran a file called "Guard.tmp" from the Explorer.exe DLL add-ons. But one mistake made by the creator of this VX2 variant was not using an official looking name in the publisher field so it stood out like a sore thumb in the Autoruns list.

So now you have a very effective way of hiding your program from the user and keeping it running at all times. But let's say you want to have a backup in case your hijacked DLL gets replaced by the latest Windows update. Another great feature of Autoruns is that it will show you empty locations as well as the ones that contain programs to run at start up. Examples include HKCU\Software\Microsoft\Windows NT\Current ➥Version\Windows\Load and HKLM\Software\ ➥Microsoft\Windows\CurrentVersion\Policies\ ➥Explorer\Run. These locations are not shown in MSCONFIG and will get past the average user with no problem. It will also evade the less experienced techs who are trying to remove the bugs in a machine. Now let's say that you run both methods. With the DLL and the little known registry entries, chances are your program will never be detected or fully removed. Of course, as Forgotten247 mentioned, there are programs that will monitor for registry changes so keep that in mind. Another method of running a DLL at startup would be to drop it into the Winlogon notifications section of the registry located at HKLM\Software\Microsoft\Windows NT\Current ➥Version\Winlogon\Notify, although this location is checked by many of the spyware removal tools such as Option Explicit's great tool called VX2finder. It is an effective way to run a DLL at every startup. Chances are if you use any or all of the methods described here your payload will be running every time the user starts their machine. Also from experience most repair shops (in my town anyway) will not try to fix the problem outright when a person brings their machine in to be fixed. Most of the time they will simply format and start over so chances are the user will never know that you had control of their machine.

Shoutz to [Isepic], Cratchet, J Ruz, Hippy Baley, Petey Pablo, and Zulupapa.



Exploits

by AOnRkjk=

In the letters section of 21:4, Citron mentions an SQL exploit. I thought an article providing some further explanation might be appropriate since I haven't seen one in *2600* yet.

SQL (Structured Query Language) provides a standardized syntax for querying databases. It is implemented in databases from various vendors and is parsed by the vendor-supplied database drivers. The syntax includes the ability to supply variables, referred to as "host variables." If you've ever seen question marks ("?") in an SQL statement or a call to a stored procedure, that is one of the ways to provide placeholders for the variables.

Now let's say you need to allow users to log into a web site with a username and password. The program needs to obtain these variables from a web form, store them as strings, then query the database and return a user ID or a "not found" condition. The values of the program variables need to be passed to the database. Therefore, the parameter list in a call to the database driver includes both the SQL statement to be executed and an array containing the values of the variables.

When the SQL statements are embedded in a program, all this happens pretty much automatically. For example:

```
#sql [connCtx] {
     select userid into :userid from
➥users where username = :username and
➥password = :password
}
```

By coding it in this manner, the SQL statement will be parsed as it was intended by the developer. Whether this SQL statement is parsed at compile time or run time, any data in the program's "username" and "password" variables will be compared to the values in the database. If

there are any special characters or other invalid data in these fields, it is likely that those values will not exist and the database will return a "not found" condition.

So if the developer has this much control over how an SQL statement is parsed, where's the weakness? Let me give you an example from personal experience.

One night I got a call from a coworker who was on his way into work and wanted some assistance. He had been called in to restore a database because it had been discovered that all of the rows in the table had been updated with bad data. This should not occur, since programs should only be updating a few rows of this table at a time. My guess was that this had probably been caused by a single SQL UPDATE statement, and so I suggested that before doing anything else we should bring up the database monitor and check the page that shows the SQL statements that have used the most system resources. This might allow us to identify the errant SQL and determine why this happened in the first place. As it turned out, it allowed us to run another update to reverse the errant one and avoid doing a restore (and losing all of the other updates done earlier that day).

In this case, the intent of the update was to change some numeric values in a specific row. In the past, we might have coded the UPDATE statement like this (this is a simplification, showing only two fields being updated):

```
#sql [connCtx] {
     update tbl set amt1 = amt1 - :val1,
➥amt2 = amt2 - :val2 where rowid = :rowid}
```

However, our company started switching to "dot Net" a couple of years ago, and this application had been developed in this new environment. In this environment, code equivalent to the UPDATE statement above might be:

```
cmd = db.CreateCommand(
     "update tbl set amt1 = amt1 -
➥@val1, amt2 = amt2 - @val2 where rowid
➥= @rowid"
);
cmd.Parameters.Add(New SqlParameter
➥("@val1", SqlDbType.SmallMoney);
cmd.Parameters("@val1").Value = val1;
➥cmd.Parameters.Add(New SqlParameter
➥("@val2", SqlDbType.SmallMoney);
cmd.Parameters("@val2").Value = val2;
cmd.Parameters.Add(New SqlParameter
➥("@rowid", SqlDbType.VarChar);
cmd.Parameters("@rowid").Value = rowid;
db.ExecuteNonQuery(cmd);
```

As you can see, the code is now a bit more cumbersome, especially if there are a lot of columns to be updated. As a result, a developer may be inclined to take a shortcut and, taking advantage of the string concatenation operator, code it this way instead:

```
cmd = db.CreateCommand(
     "update tbl set amt1=amt1-" & val1
➥& ",amt2=amt2-" & val2 & " where
➥rowid='" & rowid & "'"
);
db.ExecuteNonQuery(cmd);
```

So let's examine what happens when a user enters a positive amount ("123") for "val1" and a negative amount ("-456") for "val2" in an attempt to update a single row (rowid='789'). After the concatenation operations, the SQL passed to CreateCommand will look like this:

```
update tbl set amt1=amt1-123,amt2=amt2--
➥456 where rowid='789'
```

In SQL, comments begin with two consecutive hyphens ("--"). Since comments can be ignored, the UPDATE statement above is equivalent to:

```
update tbl set amt1=amt1-123,amt2=amt2
```

Without a WHERE clause, the result of the UPDATE statement is to subtract 123 from every "amt1" in the entire table (as well as replace every "amt2" with the same value). These particular input values have caused the SQL statement to be parsed and executed in a completely different way than what was intended by the developer!

To provide a similar example for an SQL statement that uses strings rather than numbers, let's revisit the exploit mentioned by Citron. Let's say the SQL statement is constructed like this:

```
"select userid from users where
➥(username = '" & username & "') and
➥(password = '" password & "')"
```

Now if for both the username and password fields, you enter this:

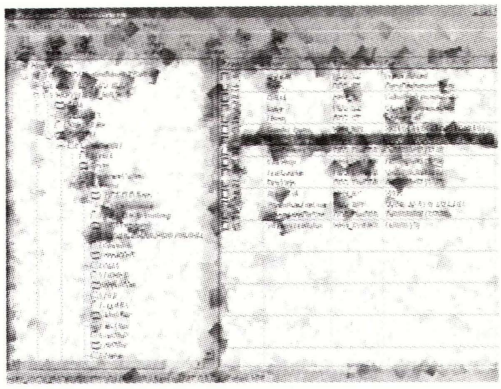
```
' or '' = '
```

the resulting SQL statement becomes:

```
select userid from users where (username
➥= '' or '' = '') and (password = '' or
➥'' = '')
```

Executing this SELECT statement will return all of the rows in the "users" table. Therefore this form of the exploit may take a long time to execute and will work only if the SELECT statement does not time out and is followed by code that retrieves the first row returned and discards the rest. If the SELECT statement had instead been coded as a single-row SELECT INTO, the database would have simply returned an error. In this case, the input would need to be constructed more carefully, so that the userid for only one user was returned.

Hexing the Registry



by divarin

This article covers editing the system registry without the convenience of the registry editor so as to bypass access restrictions. For my purposes I wanted to turn off and on various services such as the messenger service but you can use these techniques to make just about any change you desire.

The heart of any Windows based system, whether you're talking about win9x, NT, 2K, or XP lies in the system registry. The registry is where just about all system settings are stored as well as settings for most programs running on the system. This article will not go into too much detail on various registry keys because there's already plenty of knowledge out there on this matter.

It all started for me at work. I use putty to SSH into my home machine from work, but I like to cover my tracks so I would go into the system registry and remove the key cached by putty, saving it into a .reg file on a floppy disk. Then the next time I would go to use putty I would just merge that .reg file's info into the registry, use putty, then delete the keys again. Even though the keys themselves would not be enough to decrypt the data packets of my SSH session or to gain access to my home machine, they were evidence that I was running a program that wasn't "approved" by the admins.

This all worked well until one day I tried to run regedit only to find that I was stopped by a "Registry editing has been disabled by the system administrator" error. Later I learned that I was the only employee to have this restriction. I knew then that a game of cat and mouse had begun between me and one of the admins. So the first thing I needed to do was find a way to edit a registry value without using regedit.

It must be possible, since putty is able to cache the key into the registry and putty doesn't have any more access than I do. I could go on and on about my trials and errors but it's time to get to the meat of the article.

The system registry files are kept in two places: NTUSER.DAT is kept in the "c:\documents and settings\{username}" directory and all other registry files are kept in c:\{windows}➥\system32\config. (Replace {username} with your username and {windows} with the name of your Windows directory - WINDOWS, WINNT, WINXP, etc.)

Turns out the key I needed to change ("DisableRegistryTools") was in NTUSER.DAT. It's a user specific setting, right? Like I said, all of my coworkers could run regedit, though where I work I'm the only one who knows what to do with it. Well, in my corporate setting these XP boxes use a logon/logoff script system that copies your user specific settings (ntuser.dat, desktop background, My Documents, MSIE settings, cache, history, etc.) to a server elsewhere, then when you log back on these settings are copied back so that when you move from one machine to another your settings move with you. This turned out to be a huge advantage to me because you can't just edit a file that's in use and NTUSER.DAT, like all registry files, was always in use.

So I tracked down the offline copy of NTUSER.DAT (meaning the copy that was *not* in use now, but saved on a remote system) and I was able to use XP's dos-like editor (edit) to unlock the registry:

```
C:>X:
X:>ATTRIB -H NTUSER.DAT
X:>EDIT /70 NTUSER.DAT
```

Let me talk about EDIT /70 for a little bit. It's important! The /70 means a) this is a binary file so use ghetto hex editor mode (shows value of each character in the bottom right corner of the screen) and b) limit to 70 character per line. What's important is that on *most* systems this file will be too large to load into memory. If this is the case you will be presented with a warning when you enter the editor. If edit was unable to load the whole file, forget about editing this way or you'll end up corrupting the registry. You'll need a real hex editor (such as ultra edit).

What I did at this point was look for the string "DisableRegistryTools" and when I found it I simply changed the "T" in Tools to an "F." (Initially I was thinking the joke would be a boolean, T/F, True/False. It wasn't until later I realized it said "Fools.") I figured if XP couldn't find the key it would have to set it to a default value, which should be 0 (not disabled). And I was right.

Then what I did was set the file to read only so that when I logged out the logoff script would not be able to overwrite the file with the current settings:

```
X:>ATTRIB +R NTUSER.DAT
```

Logged out, back in, tada I could run regedit again. However, the next day I was unable to keep that file +R so they must have added "ATTRIB -R X:\NTUSER.DAT" to the logout script. Well, I could just not log out or I could unplug the ethernet cable while I do. But what's interesting is that they didn't disable the registry tools again.

I was able to remove my putty SSH keys. But then I started poking around in the rest of the registry thinking "You know I always hated that messenger service - it gives me a dialog box that says 'Your document has printed successfully' every time I print something."

Most NT/XP administrators administer their systems using point and click GUIs. You ask them how to turn on or off a service and they say to click on control panel, administrative tools, services, etc. But at this level the OS really pays attention to the user's rights and policies so therefore I was unable to disable the service at this level. So I dropped to the next level, somewhat like the DNA level, regedit. I found the key "Messenger" under "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger" and the DWORD value "Start" currently was set to "2." What I wanted was to change that to "4." (2 means automatic, 3 means manual, and 4 means disabled.)

Let's walk through the process. When we try to change the value here to "4" we get an error, something like: "Unable to save changes." Apparently our access restrictions are still taken into consideration at this level so it was time to drop down another level. This is somewhat like the atomic level and to get there we're going to need two tools: a hex editor and a Windows 2000 CD-ROM or boot floppies.

What we need to do is hex edit the c:\windows\system32\config\system file, but you can't edit a file that's in use remember? Unlike NTUSER.DAT this file is not copied to another system at logoff so there is no offline copy of it... yet. This is where the Windows 2000 CD-ROM comes in. We need to boot up to the recovery console in the Windows 2000 setup program to make a copy of the system file.

Why Windows 2000? A long run-on paragraph can explain this but since I'm a nerd I'll use a chart instead:

CD-ROM	***Why we can't use it***
Dos/Win9x	*No NTFS support*
Win XP	*Asks for admin password*
Linux	*Limited NTFS support, not enough to do what we need done*
NTFSdos Pro	*Supports NTFS4 but not NTFS5 which is used in XP*
Win NT4	*Same problem as NTFSdos Pro*
Win2K	*No reason!*

If you don't have a Windows 2000 CD-ROM, don't fret. You can get the boot disks (requires four floppy disks) from www.bootdisk.com.

Reboot the machine and boot off either those floppies or the CD-ROM. I'll leave it up to you to deal with the boot sequence in case the admins have set the system up to not boot from CD or floppies. There are ways around this by getting into the CMOS setup but that's out of the scope of this article.

Now when given the choice say (R)epair, then (C)onsole, then (1) c:\windows (or WINNT, whatever):

```
C:\WINDOWS>MD \REGHACK
C:\WINDOWS>COPY SYSTEM \REGHACK
      1 file(s) copied
```

(you'll notice if you try to copy *.* it won't work. You must copy one file at a time - strange...)

```
C:\WINDOWS>EXIT
```

OK, that's one part down. Keep that Win2K CD handy. You'll be needing it soon. Boot back into XP and load up your favorite hex editor. In this article I will use UltraEdit-32 because it's nice but any hex editor should do as long as you can do ASCII searches.

Load up your hex editor and use it to open the c:\reghack\system file. Yeah, it's an alien language, isn't it? I've used hex editors (and in my childhood a sector editor) to alter string values before but altering numeric values is a bit of a trick. Let's continue with my example as we try to turn off the messenger service.

Do a search for "messenger". Be sure you're searching ASCII, not hex. You'll get a match. In fact, repeat the search and you'll see you get a lot of matches. I counted eight on my system. So how do you know which one you really want to edit? Load up regedit and use it as a "map" to navigate your way around the binary data that is the system file. Look at the key:

(Note: some lines cut off to save space in this article)

```
NAME              TYPE          DATA
(Default)         REG_SZ        (value not set)
DependOnGroup     REG_MULTI_SZ
DependOnService   REG_MULTI_SZ  LanmanWorkstation NetBIOS ...
Description       REG_SZ        Transmits net send and ...
DisplayName       REG_SZ        Messenger
ErrorControl      REG_DWORD     0x00000001 (1)
ImagePath         REG_SZ        %SystemRoot%\System32\svch...
ObjectName        REG_SZ        LocalSystem
Start             REG_DWORD     0x00000002 (2)
Type              REG_DWORD     0x00000020 (32)
```

The DWORD value we want to change is labeled "Start". The value it is now is "2". Let's go back to our hex editor and look at the first match:

```
00056d50h: 4D 65 73 73 65 6E 67 65 72 00
➥0A 00 48 00 4B 00 ; Messenger...H.K.
```

We don't see "Start", or "Type", or "ErrorControl" or anything else like that near here so let's move on to the next match (for this example I will use ?'s to replace strange extended ASCII characters that are font specific):

```
                01 02 03 04 05 06 07 08 09
➥10 11 12 13 14 15 16
000bca10h: 82 00 00 00 09 00 00 00 4D 65
➥73 73 65 6E 67 65 ; ,.......Messenge
000bca20h: 72 00 00 00 00 00 00 00 30 FF
➥FF FF 76 6B 04 00 ; r.......????vk..
000bca30h: 04 00 00 80 20 00 00 00 04 00
➥00 00 01 00 00 00 ; ...? ..........
000bca40h: 54 79 70 65 00 00 00 00 08 00
➥00 00 28 BA 0B 00 ; Type.......(?..
000bca50h: E0 FF FF FF 76 6B 05 00 04 00
➥00 80 02 00 00 00 ; ????vk....?....
000bca60h: 04 00 00 00 01 00 00 00 53 74
➥61 72 74 00 00 00 ; .......Start...
```

And there it is! Only three lines below "Messenger" you see "Type" and two lines below that, "Start". Now the trick is finding the value of "Start". DWORD values are easy to spot if you know what you're looking for. And what you're looking for is hex character 80, which is the euro look'n symbol. Here it's on 000bca50h as the 12th byte.

Notice how the value for "Start" actually appears before the word "Start." Strange, huh? The 80 character means that this is the start of a DWORD value. DWORD is Double Word. A double word is two words, a word is just an expression for two bytes. Therefore, a double word (DWORD) is four bytes. So the next four bytes represents the value of "Start." This example shows "2" as the value because the messenger service is turned on. You might think that a value of "2", represented in four bytes would look like "00 00 00 02" but that's thinking like a human. Don't do that! Computers read left to right regardless of whether they're reading numerical values or words. Well "2" in hex is "2" in decimal, and "4" in hex is "4" in decimal. So to turn off the messenger service, simply replace the "02" with "04" and then save the file.

Now just use your Win2K boot CD/floppy to get back to the recovery console, make a backup of the registry before you mess things up, and copy over your changed system file:

```
C:\WINDOWS>COPY SYSTEM SYSTEM.BAK
C:\WINDOWS>COPY \REGHACK\SYSTEM .\
Overwrite(Yes/No)?: Yes
C:\WINDOWS>EXIT
```

That should do it. The messenger service should now be disabled. You can use this technique to make any change to the registry you want but know that some keys are in different files (system, software, ntuser.dat, etc.). Finding the values is the real trick. Also, if you are looking for a string value, take note that each character is separated by a 00h character. Strange.... So if you are doing a search, be sure that regular expressions is turned on and add ?'s between each character:

```
s?o?m?e???s?t?r?i?n?g???v?a?l?u?e
```

P.S. Yes, I have attempted to load my copied registry files into the registry editor with the /L and /R options but that trick doesn't seem to work anymore. Perhaps it was taken out in XP or perhaps it only works on exported key files.

STOP!

Urgent message. Go directly to page 61. Do not resume reading until you have done so.

Thank you, your cooperation has been noted.

- the 2600 Easter Bunny

Words from You

Devious Plots

Dear *2600:*

Here's something fun to try at the Wal-Mart U-scan checkout machines. During checkout, input coins *after* inserting a bill. As it is trying to compute the change it needs to dispense, it gets confused and it gives you your item nearly for free. It even gives you a legit receipt. Here is an example: Let's say I'm buying an item for $16.47. I scan the item as usual and continue to the "Pay with Cash" screen (we are going to pay with a $20 bill and 47 cents). Insert your $20 bill and immediately after inserting the bill begin inserting your coins. The machine will say something like "Do Not Insert Change At This Time." (We only inserted two pennies before this happened.) On the screen it will say "Change Due: $20.00." The transaction will complete and if you did it right it will give you $20 in change! It will print a receipt that says you paid the correct amount and received only $3.53. Wow. This is a major flaw in the software of the machine and I suspect it affects all U-scan machines in Wal-Mart. This was not just a fluke and is repeatable. I would be interested in knowing how many other readers are successful in trying this. Now of course, I don't condone theft and I don't plan on doing this more than is necessary to intelligently inform Wal-Mart of this major software screw-up. Props to my girlfriend for finding this flaw accidentally and showing it to me.

anonymous

Oddly enough, this little trick often gets the exact same result from human checkout units. Perhaps confusion is the common ground between man and machine. We'd be curious to see if this works on all such machines. It will certainly cause one hell of a commotion if it does.

Dear *2600:*

This is a cute little exploit that allowed me to get some free games on my Nokia 3100.

Up here in Canada, I am on a prepaid phone plan with cellular provider Fido, which was recently acquired by Rogers Communications (the monopoly of Canadian cable/Internet service). On my Fido phone, there is a menu on the front screen which reads "browser." By hitting browser and waiting a few seconds, you will be logged onto the Mobile Internet (WAP). There you can view things like your horoscope, download wallpaper, ringtones, games, etc. I realized once that when downloading a game from a Gameloft website, I wasn't charged for it. After further exploring the matter, I discovered that Gameloft's games had a silly system of distribution, just begging to be abused. The game is downloaded by the user and after the download the user hits "Done." Then they will be charged for the game. By hitting the Red escape button on the phone you simply escape that screen and you aren't charged at all. I was able to get over $100 in free games using this method! It only worked with Gameloft games, not with any other company, and the exploit has recently been patched up. I'm not sure how many other people used this method but it was fun while it lasted. Keep up the good work!

Shah Chopzillian

Random Questions

Dear *2600:*

I have an interesting article about a free voice messaging service in mobile phone companies.

I would really like to get that free shirt and the one year subscription. Because I'm in an Asian country I might have a problem getting that free stuff. Please tell me whether you'll be able to send me those things or not.

B.H.K. Chanaka
Sri Lanka

If we use an article of yours, we'll send you a free shirt and a one year subscription. If you're in a far off land, that deal still stands. If there's some sort of difficulty with mail delivery in your part of the world, there's not a whole lot we can do about that. We're only able to strike fear into domestic postal employees.

Dear *2600:*

Would this be the correct address to write to if I had a question about hacking?

CalebLeo1

Depends. If that was the question, then yes. For all others, no. We hope that helps you.

Dear *2600:*

Would you please tell me the deadline for submitting articles for the next issue of *2600?* Also, you do not need to be a subscriber to submit an article, correct?

Steven

Don't worry about the deadlines as they're always coming and going. Just submit your stuff to articles@2600.com. Anyone can submit an article but be advised that if it's accepted you will become a free subscriber for a year. The only way to prevent this is to not give us an address when we contact you after it's printed.

Dear *2600:*

What file format should I use to submit an article that contains pictures?

Jeff

Try to submit the text in straight ASCII and attach the pictures as TIFs, GIFs, or JPGs. We're usually able to read most formats but articles have been thrown out because they were too much of a pain in the ass to translate. So the best rule is to keep it simple. You can also submit it in a couple of different formats if you're unsure which is best.

Dear *2600:*

I am an applied computing student located in the UK. And I am very much interested in writing articles for *2600.* I wish to know what kind of articles you demand or are looking for at the moment.

Henry

We demand articles that are thought provoking and which cover areas of hacking that haven't really been covered before. This can include ways of hacking something that you're especially good at, additional information on a topic that we've already touched upon, or even theoret-

ical hacking. Any form of technology is eligible and sometimes it doesn't even have to involve technology at all. Above all else, write your piece from the perspective of a hacker. We think if you glance through this and a few other issues, you'll see quite a few examples of this.

Dear *2600:*

If our article fails to get into *2600,* are we able to send it to another publication for attempt at publication there?

Andrew

Of course! The article remains your property and you can do what you wish with it. Other publications may make you agree to give up these rights however. All we ask is that you not submit material which has already been published, either in print or on a web page. We don't care what you decide to do with it after it hits our pages.

Dear *2600:*

Hey there, enjoy the magazine, long time reader, occasional meeting and HOPE attendee.

From my reading of *2600* I think I have gathered that you are opposed to repostings of articles in their entirety in other places without giving credit to the original source. I was reading the latest issue (22:1) and looking online and found the following page: http://forevergeek.com/articles/unlocking_the_power_of_wap.php. It seems to be posted by the same individual who submitted it to the magazine (Josh D.) but doesn't mention that it appears in *2600.* Not sure if you have any kind of policy against that since it is the original author but just thought you should know. Thanks for the good magazine/conferences. See you at the next HOPE.

George

We appreciate the gesture of ratting someone out for us but our policy remains that the author can do whatever s/he wishes with the article they've written. Naturally we'd prefer there to be a pointer of some sort but it's ultimately up to the writer. Again, this would be an issue if it were on the net before we printed it as we don't want to be publishing previously available material, with the exception of articles translated from other languages.

Dear *2600:*

Recently I bought the newest issue of *2600,* 22:1 to be exact. On the first page after the cover labeled "Details" I discovered in small gray text above the phrase "Potential Vulnerabilities in Shared Systems" the word "hopenumbersix." It was placed exactly over the word vulnerabilities and I wasn't sure if it was an Easter Egg or something that would earn me a *2600* bumper sticker (or something corny and cheap like that) or if it was a misprint. I searched 2600.com and googled it and got nada. If you could explain it to me, it would be great.

Duciniti

Perhaps you ought to search again.

Dear *2600:*

Fred (Derf/Admin99) of *2600* asked me to write an article and said the deadline for this next quarter is June 19th. I guess I was to give it to him and he was going to submit it on my behalf, however he seems to have gone MIA and the time is close upon us here. His cell phone seems to be disconnected and he hasn't been reachable on AIM. How do you suggest I proceed?

Dave

Proceed by never believing anyone who says they're affiliated with us and who offers to be a middleman. They're most likely working against us. And as you can see, they often disappear when their past catches up with them. (Our hands are clean on this one.)

Dear *2600:*

First off, thanks for the great mag. Me and about five other friends have a club where we read *2600* and if we find an interesting article we try it. But my question is: Who is the man holding the briefcase with the biohazard symbol on it in the last two issues?

Black_Angel

We wouldn't be highly regarded in the privacy community if we just gave out someone's info like that. Especially without negotiating a price first.

Dear *2600:*

I just picked up 22:2. I absolutely love the article "One Step Forward, Two Steps Back" on page 4 and 5. Would it be OK with you if I copied that article and posted it on a few bulletin boards? Consider it free advertising or a way to help spread the message.

Jeff

This is perfectly fine as long as you give attribution and a link.

Security Holes

Dear *2600:*

I've read several of your magazines so far. I will admit I am not actually much of a hacker, but by reading your magazine I have become a little more aware of things that could be exploited. I was at the airport the other day and I was helping my grandparents get to their airplane by pushing their wheelchairs. I wanted to push them to the gate so I was given a special ticket. The ticket allowed me to go with them, while not allowing me to board a plane. There was one problem though. As I was going through security, they only glanced at my ticket. Suddenly I realized that one could take a picture of the ticket and edit and use it again to get back to the gate area, provided the edited copy was well made and the checker didn't ask for the disabled person you were helping. I'll leave it to you to speculate about how this could be dangerous. Even more surprising, when I left the airport no one ripped up the ticket or had me throw it away. I could have taken it home, scanned it, and edited it to produce numerous tickets such as this.

The second thing I noticed were the payphones. I had an urge to fool around with the phones, but did not for fear that I would look like an idiot. However, I noticed that some of the individual areas where the phones should have been had been covered by a sheet of metal that was attached with some sort of weak adhesive. With relative ease, one could pull the sheets off the wall and get a hold of the cords that the phones had once connected to. Again, I'll leave you to speculate about what one could do with a hole in the wall and potentially the cords that had once connected to the payphone. Thank you for your time.

Anonymous

If they were the old fashioned Bell payphone lines, all you would be able to do at most would be to use that line in payphone mode. If it was a COCOT line, there might be some other possibilities. But this is so frequent a scenario that it's not that big a deal. Also, you would likely draw quite a bit of attention by pulling metal sheets off walls and connecting your instruments to the wires.

As for your first scenario, this is probably something the airport people would take seriously. But remember

that it wasn't too long ago when going to the gate with a passenger wasn't anything to be concerned with. We're not convinced that "world events" have changed anything but the paranoia level in various officials. After all, anything you could do at the gate if they let you through without a ticket could also be done simply by buying a ticket. So where exactly is the increased security? We suspect it resides in a few minds but not in many other places.

Dear *2600:*

Hello! I thought your readers might be interested in knowing how lax Cox Communications' security practices are. I occasionally call on my mom's behalf when she has Internet problems. Every time the automated system prompts me for the telephone number and last four digits of the primary account holder's Social Security info. I always enter 1234 as the latter and no one's ever pressed me for the real information. The last time I called, the human I finally spoke to asked me for the name, address, and SSN of the primary account holder. I gave him the first two and told him I didn't know the last one, but that didn't stop him from telling me all manner of things about the account.

Anyway, I just thought you folks might find that enlightening.

KJ

Just for the fun of it, see if your mom's SSN actually does end in 1234.

Observations

Dear *2600:*

I'm avid reader and a former subscriber. I'm debating whether or not this is newsworthy to you but I'll pass it along anyway.

Brief background - I'm enrolled in a Masters program called "Information Assurance." Our professor (really just an adjunct) asked us to make introductions to the rest of the class (it's an online course). I mentioned my interest in *2600* and this is how my instructor replied:

"You might recall from my brief biography that I was involved in security at US Sprint in a past life. I too was an avid reader of *2600 Magazine* and was an undercover member of the *2600* club as were ten of our regional security managers. During the years 1988 through 1990 we executed over 180 search warrants along with the United States Secret Service on various hackers who were either members of, or purported members of, the *2600* and other global hacking organizations. We seized a whole bunch of computers and scared the living daylights out of a bunch of hackers and their friends and parents. The defendants were charged with hacking, distributing stolen credit cards, distributing stolen telephone authorization codes, and illegally reselling telephone services. By the way, every one of them faced a criminal prosecution and was either convicted or plead guilty as charged.

"A friend of mine once admitted to reading an insurgent group magazine on a regular basis. When I asked him why he did that he said, 'I think it is important to know what the enemy is thinking.' I understand your perspective."

john

Wow, we're being likened to insurgents now. Can it possibly get any better?

Dear *2600:*

On a recent trip I had a layover in Houston. While at the airport there, a lady came over the PA system and said "Threats, suspicious activities, and inappropriate jokes will not be tolerated and will result in jail time." I can understand the first two, but we can't tell jokes now? Yes, you read that right; it's apparently illegal to tell off-color jokes in an airport! Anyone know what happened to the First Amendment?

On the plane leaving Houston, I took the opportunity to experiment with the phone in the back of the seat in front of me (a Verizon service). I had noticed that you can reach the operator for free (normal calls require a credit card transaction). Having already forgotten about that encouraging message over the PA at the airport, I told the guy next to me it would be funny to dial up the operator and tap out SOS in Morse code. He said you had to pay to reach the operator. I showed him differently, and once I was connected to the operator I typed out SOS three times. Then I held the phone up to my ear. To my horror, I heard "Stay on the line for 20 seconds and we'll land the plane." I hung up and freaked out for the next 45 minutes.

I know sending out an SOS in a post 9/11 world was stupid and immature, but this system seems incredibly ludicrous to me. I'm guessing this "feature" was implemented after 9/11 since many of the passengers were smart enough to call home using the same type of phones. It must have been created under the guise of safety, but I doubt it could ever protect anyone since I don't know many people that can translate SOS into Morse code, and I haven't found anyone else that knows about this setup. One final concern: How did Verizon come to control which planes stay in the air and which ones are grounded? Aside from incompetence and virtual bribery, why would our government entrust our safety to a phone company?

Dr. Apocalypse

There's really nothing new about the joke thing. But by "inappropriate," they mean jokes about security, hijacking, etc. that might make people really nervous if there's the perception that you may not be kidding. This has been the policy for decades.

As to what you heard, you didn't mention if it was a recording or a human. We'll assume it was the latter in which case we'd bet it was an operator attempting to ascertain whether or not this was a true emergency. By giving you that warning, it sure got you to stop in a hurry. Verizon obviously doesn't have the power to land planes but after receiving an SOS signal from an aircraft, they're certainly in a position to pass that along to the relevant authorities. We trust you learned a valuable lesson here and hopefully kept many others from venturing down this path.

Dear *2600:*

Just a comment on AT&T Easy Reach 800 service PINs: The two digit PIN is not meant to provide security by preventing calls from unauthorized users. Instead, it is meant to keep people from accidentally getting in. People who get a personal 800 number usually use it as a way for their family (say, kids in college) to be able to reach them easily. If your personal 800 number is one digit different from, say, an airline, a two digit PIN will be very effective in avoiding charges for hundreds of accidental one minute calls (and it prevents your phone from ringing at 4 am). A more secure PIN (i.e., longer) would make it harder for the people you want to call you to remember how.

5+3v3 D4v3

Dear *2600:*

It seems that Miss Hillary Clinton has decided to join the ESRB against RockStar Games' inclusion of "adult content" in their recent Grand Theft Auto game (San Andreas). Now personally, I think that someone writing a computer game should be allowed to put whatever they want in that game. Sex, drugs, rock and roll, whatever. But there's supposedly a "hot coffee mod" that allows you to play a sex mini-game which would supposedly cause the game to require an AO (adults only) rating from the ESRB. (Having looked at the screenshots, I doubt this. All "actors" are fully clothed.)

Now I wouldn't really care about any of this, were it not for the fact that Rockstar Games has decided to deny putting that content in their game. Instead, guess who they've blamed? Yep, you got it. Hackers. Rockstar Games is blaming hackers for breaking into their computers and modifying their source code to GTA:SA and adding a sex game.

This is ridiculous! First of all, Rockstar Games is a software company and, knowing software companies (having worked in a few myself), they're likely to keep a somewhat good security setup alive at all times. They're developing multi-million dollar software and they'll want to make sure it isn't stolen/altered. In addition, there is probably someone watching their servers, checking logs, and doing maintenance. They should have seen *something* that would have alerted them to a "hacker" break-in.

Now let's assume that all of this is false. Rockstar Games doesn't care about security and leaves their server open for all to break into. (We could just blame them for being idiots, but we're not going to do that.) Assuming that there is no security involved, let's say someone comes in and tries to reprogram the software. (According to Rockstar Games, hackers went to "significant trouble to alter scenes in the official version of the game.") So some "hacker" went in and started reprogramming the software? Let's see what this entails.

First, they must break into Rockstar Games' website. Let's pretend this takes them about one month, for enumeration, exploration, penetration, gaining sufficient rights, etc.

Next, they must search the computer for the software they are looking for. About ten minutes' search, tops (assuming it was located on the computer they happened to break into).

Once they've found the software, they will either 1) download the source to their own computer to work on it, then upload it again when they're done, or 2) modify the software directly from the other computer. The first choice is unlikely as their version would be detected by any CVS out there (or another programmer). There would be too many ways for it to be discovered (assuming that Rockstar Games is an efficient and quality game programmer, which they must be based on their success). The second choice is also unlikely because in order to modify the software directly on the remote computer they would have to stay connected and risk being caught, and they wouldn't be able to use a specialized programming system, resorting instead to something like vi or emacs.

Once they have the source code they would have to orient themselves with the software and how it works and then modify it. This is because chances are each programmer works a little differently, and currently the hacker does not know how the software has been organized. So let's say it takes one month to sufficiently figure out how everything works and find the specific places they need to modify.

Next, they have to create graphics (for the status messages and skill bar and whatever else was added). Let's put this at a week (extra time to make it look right and fit in with the rest of the game). We're at two months, one week, ten minutes so far.

In addition to new graphics, they will have to create new animations and new scenes and areas and controls in order to allow the system to know how to properly display and handle the little mini-games. I'm going to put this at two months, not including upload time and time taken to cover tracks.

Assuming they are able to modify the software, they would then have to find out what CVS is being used and submit their changes before they become out of date. I personally don't know as much as I should about CVS, so I'm not going to inquire about the difficulty of this task. Let's assume it's easy. Cinch. No challenge for a hacker to put this in the code. Let's say it takes all of twenty minutes, most of it spent just finding the CVS, not submitting to it.

Now that they have effectively broken in, modified the software, and submitted it to the CVS, they can erase their logs and go. Thirty minutes to erase any traces of their break-in and they're gone.

Total elapsed time: Four months, one week, one hour.

Now that doesn't seem like much... but chances are most hackers would be deterred by time alone. Second, even if a hacker *did* get in, quality control should have found the modified code. Isn't it amazing how a hacker just broke in and wrote completely bug-free code, modifying the software without causing any problems or discrepancies?

All in all, I think the chances are much higher that either 1) The maker of the "hot coffee mod" made the scenes himself and added them with the mod, or 2) Rockstar Games did, in fact, include the software in their game and are blaming it on hackers.

I would like to know what you guys think about the whole matter.

theXorcist

We really expected a more enlightened reaction from them. To just blame it on hackers is the equivalent of accusing hackers anytime something goes wrong with someone's computer and important information is lost. We see that all the time. It's an easy way to point attention away from one's own mistakes and failings. In this case, it seems quite apparent that the mod was intentional on at least one of the developers' part and that the people on the executive ladder didn't know about it. So rather than turn attention to themselves and risk the wrath of the Religious Right, it was far easier to blame someone nebulous who would never be able to be found anyway and who was already demonized in the mainstream. We just don't know why they felt it was necessary. Considering the game is about stealing cars and evading police in the first place, we can't imagine why a little sex would cause such a scandal, except of course for the element of fear the politicians and businesses currently operate in. But we definitely expected better from these guys.

Dear *2600:*

So now we're putting a price on someone's life? I'm been reading the headlines crying over Sven Jaschan's sentence being too easy. Well maybe, maybe not. Yeah, he was a pain in the ass, but so is the kid tagging and we're not thinking about killing him like the fucking moron John Tierney wants to do with hackers. I can't understand why so many people are grabbing their torches and pitch-

forks to take part in the modern witch-hunt. I've long thought the cost of downtime companies claim is ridiculous, especially when considering my own spending habits. How many times have we tried to order something, had trouble hitting the site, and just come back later? I know I have. So how can the company claim lost sales? They sure as hell can't claim labor costs, since most of us admins are salary. So again, how much are companies actually losing? The real problem is I'm running into more and more people who agree with Tierney's attitude. But back to my original question: is our society really so damn greedy that we're willing to say once someone exceeds a certain damage threshold they're eligible for the death sentence, which is essentially putting a price or worth on a human life?

And to all the morons that agree with Tierney: if your data is worth more than a human life, why the fuck didn't you back it up?

-ht

We somehow find it hard to believe that anyone would advocate death for such a thing. We believe the now infamous New York Times opinion piece by Tierney was presented as a tongue in cheek solution in response to what some saw as an overly mild sentence (21 months of probation) for the creator of the Sasser worm. We don't think there's anything at all wrong with creating a worm. Releasing it however is a different matter. But the fact boils down to this: it shouldn't be so easy to cause these kinds of problems in the first place. And there's no way it should permanently affect anyone if they take the simplest of precautions. We use prison in our country as a solution to every problem. It doesn't even work most of the time. The Jaschan sentence handed down in Germany may have angered those crying out for blood but it won't make the net any less secure. Companies releasing products with all kinds of holes and an uneducated consumer base will be the ones responsible for that.

Dear *2600:*

I was just listening to the news (yes, I know mainstream media isn't the best source for a full, unbiased story but...) and they mentioned that legislation is in the works to allow people on subways to be randomly searched by police! How awful is that? The government is also working on having unfettered access to your medical and library records as well.

At what point does the common, everyday person - the majority - draw the line and say "Hey, I thought I had a right to privacy. Why am I being needlessly inspected? Why does the government have a right to just look at my private records?" and begin fighting to protect such simple and fundamental liberties? The loss of our civil liberties is reaching an atrocious proportion.

On a side note (this idea is almost worth a separate letter submission), why doesn't someone who is well versed in laws pertaining to civil liberties write a nice, thorough article/list for *2600* about what we do and do not have the right to do? I, and I am very confident many other *2600* readers, would very much enjoy and find extremely useful a fairly extensive list of "Liberties and rights you (probably) never knew you had."

One of these would include not being forced to identify yourself to any police officer who randomly asks you for some ID. I never knew that. I am even more educated about our civil liberties than the next guy. That would make a great example for a list of this description.

I'm sure there are many other rights and loopholes we never really knew we had and enumerating some of the lesser known (depending on who you are) examples of using our civil rights not only might inform readers but might promote an extended use of these liberties that are being sadly stolen from us.

Krazy

We would certainly welcome such a submission from a credible source. And to answer your first point, people have most definitely begun to fight back against these intrusions. What hurts the most is the perception that this is not happening and that's something many of us have the power to change. It doesn't take many people fighting back and sharing their results with the world to actually have that perception changed in the eyes of the mainstream. You're a lot more powerful than you know.

Dear *2600:*

I recently went to Disneyland and noticed something interesting. Disneyland now has a bag check like at the airport. If you have a backpack, they ask you to open the pockets. The first check I went through, the lady gave a quick glance and let me pass. At first I laughed. If they were checking for bombs, this made no sense. Why be so brief? I then suspected they were checking for food, so I did a quick experiment. I put a can of soda and some chips in my bag the next day. Again the lady quickly looked at my bag and let me pass. Near the end of our trip, my sister got a teddy bear in a large box. The box had a small hole in it and as the lady checked it, she looked in the hole and gave it one shake. Why is Disneyland wasting so much money on such laughable "security?" We may never know. I just wanted to know what you guys thought of this.

By the way, great mag. I am 13 and I love it though I don't understand half of the code.

Sam

Disneyland is a microcosm of the United States. The same silly security practices they use there can also be found in many other places. It's really all designed just to give an illusion of safety. And maybe also to make us laugh.

Dear *2600:*

I recently sent an inquiry to Yankee Stadium through their website inquiring about WiFi access in the stadium. The response I got back had the word "SPAM" enclosed in brackets, as well as the words "sender blacklisted." It also had a one line response of: "We do not allow laptops into Yankee Stadium." When I wrote back asking why, I was told that: "These are our Stadium security policies" and given a link to their "security policy" page as well as a number to call if I had any further questions.

It appears that they consider laptop computers to be a "security risk." And as such they do not allow them in the stadium as well as video cameras and glass or plastic bottles.

I got no response to my inquiry as to why the subject line of my email contained the words "SPAM" and "sender blacklisted." The second reply contained a thank you for supporting the Yankees, as well as a "looking forward to seeing you at Yankee Stadium."

Now correct me if I'm wrong, but would the words "sender blacklisted" suggest that I have been placed on some list and that it is possible that I may not be able to purchase tickets to go and see the Yankees play baseball at home?

I honestly cannot see or understand how or why a laptop computer could be considered a "security risk."

Digital_Cowboy

That ban makes very little sense. But the City of New

York saw fit to ban blankets at a concert last year for the same "security reasons." It's got nothing to do with security. They simply use that word as a way of getting you to do whatever they want you to do.

You most certainly have not been put on some sort of a blacklist. That message in all likelihood was generated by your system or by one further upstream in reaction to the incoming message. To some spam filter, their message either looked like spam or their address showed up on a list. Apparently you still get mail that has been so marked which in this case was a good thing. There's also a chance this could have happened on their end and they weren't aware of it (obvious from it remaining in the subject line).

The blacklisting in question is most likely that of a third party (like the SORBS list) that someone's spam filter is set up to query. Input both your IP address and theirs to a query site like http://rbls.org/ to see where the problem may lie.

Dear *2600:*

Did you know that your hat made it into an art show of Xerox art?

http://www.meandmybadself.com/xerox/

thedave

We had no idea. They show up in the strangest places sometimes.

Dear *2600:*

Want to first start off saying I love the magazine. I was looking over this dictionary of computer and Internet Terms by *Barron's Business Guides.* And I wanted to see what they had listed for hackers. Their first two definitions were great but the third is what I have to talk about!

"1. An exceptionally skilled computer programmer.

"2. A person who programs computers for recreation or as a hobby.

"3. A person who 'breaks into' computers without authorization, either for malicious reasons or just to prove it can be done; a cracker. See *2600."*

I could not believe they put *2600* on the third term with the malicious part. So I went to see what they put for *2600.*

"A number used as an identifying code by groups of people who exchange detailed information about how to break into computers, tamper with telephone systems, duplicate credit cards, and the like, whether for purpose of preventing or encouraging these acts. There is a magazine *(2600: The Hacker Quarterly)."*

Mixfever

We're curious as to whether their business advice is as bad as their definitions.

Dear *2600:*

Dr. Ultra Doom Laser made a comment in 21:4, page 35 about a sequel to the movie *Hackers.* For your information the sequel was made in 2000 and is entitled *Hackers 2, Takedown.* It's a movie about Kevin Mitnick. Personally I thought it was a good movie, depicting social engineering. Due to copyright and other issues it was never released in the US. However, using one word out of the movie's title you can find it on the net and... well you know.

e-tipper

"Takedown" has no connection to "Hackers" and is not listed as a sequel to it anywhere. And it was finally released in the States under the title of "Trackdown" a full four years after its release in the rest of the world.

Responses

Dear *2600:*

This small deluge is in reply to LoungeTab's article in 22:1 on scumware removal. I've seen several of these articles and some reply letters in recent issues of this publication, as well as in many other articles. I have spent quite some time working for an undisclosed major retail location (where a clip-on tie is part of the standard uniform) and as such have spent most of that time removing spyware, malware, and every other ware I can think of from user PCs. In honest truth, most of the programs mentioned are our unsanctioned tools to remove most pieces of spyware, but I figured I should add my two cents for some of the tougher pieces of spyware.

First, before you do anything, be sure that system restore is off, otherwise all of this will be in vain. I have seen techs spend two hours on a single PC only to have system restore undo all of their work in fifteen seconds.

Instead of HijackThis, I actually recommend Emsi software's HijackFree, located at http://www.hijackfree ➥.com/en/, because it gives a broader list of options for removal and will actually directly reference the key in regedit if you want to manually edit the registry entry.

For removal of the most stubborn of programs, whether they simply refuse to delete or they reappear after deletion, use the KillBox, located at http://www. ➥bleepingcomputer.com/files/killbox.php, which has the ability to delete stubborn files, and to replace these files with "dummy" files so they stop propagating.

At this point, removal is simple by running the programs one after the other until you wind up with either no spyware remaining, or you have one or two still left. With spyware such as the infamous "VX2" variety, you will need to locate the "hub file" that the program runs off of (VX2 usually uses nail.exe) and replace it with a dummy, then remove the spyware afterwards. Other hijackers such as "smitfraud" (characterized by a Windows 98 looking BSOD on a Windows XP desktop) can be removed with custom scripts (smitfraud's is here: http://www.bleeping ➥computer.com/files/reg/smitfraud.reg).

Now you have removed all your spyware but there are still things to do. First, get yourself a registry cleaner of some kind (such as Norton's WinDoctor) to clean out any leftover hanging registry entries, then use a disk cleaner to clean out your temp files. Finally, be sure to reset your winsock settings, as some of the more in depth removals tend to severely damage these. Use a program like winsockfix (try http://www.tacktech.com/pub/winsock ➥fix/WinsockFix.zip) to get that repaired.

Hopefully that will take care of the more stubborn files and won't leave you with a fried system after the fact. Happy surfing, wherever you may find it.

TackGentry

Dear *2600:*

Just wanted to say I enjoyed the article in 21:4 about using steganography to detect credit card fraud. I've found it works well in restaurants and pay-at-the-pump gas stations. Using the date in your algorithm is a little tricky because the date on your statement is the date the transaction actually went to the bank that issued your card (sometimes several days after the date you used your card).

On an unrelated subject, I really like the new layout. Payphones have never done much for me but ironic photos - now *that* I can get behind. And I also dig the new font. Things seem easier to read. Or maybe that's just new car smell kicking in.

kip

Dear *2600:*

In 22:1 you mention how to make a single track magnetic strip reader. There is an easier way to make these. At a gas station/liquor store tell the clerk that the soda dispenser is out of carbonation and he will more then likely go in the back to get another bottle. While he is in the back, unplug the strip reader from the back of the computer which should be right in front of you and run out the door. Once you have about two or three of the readers you can begin to tear them apart and modify them to fit in your pocket.

forrest hoover

Yeah... that's another way. But we were kind of gearing the article towards intelligent people who wanted to learn how the systems worked, not petty hoodlums who go around stealing things and running away from people. We appreciate hearing that perspective however.

Dear *2600:*

In 22:1, you say four new pages have been added. But I count five. You added page 33! I was flabbergasted.

kingconga

Dear *2600:*

I read in 22:1 under "Utter Stupidity" something that intrigued me as I recently had a relatively similar experience with Blackboard. The letter written by Public Display was nearly correct. The systematics of Blackboard work as follows. You communicate with teachers and other students about classes, homework, and the like. That is all true. However the logging in portion was not entirely correct, although for his area it may very well be. It seems to me that it is entirely set up by the school network admin. At the school I was at, it was each student's last name, and we were all instructed to change it to something else upon our first login. That's all fine and good, but many people did not change it. At the school my girlfriend was attending at the time, they too had Blackboard and they had a much more secure login, i.e., the last four digits of their SSN.

The major flaw that I noticed in Blackboard at the time was not the login, although that was an issue they left way too open. It was the amount of info each account showed. At the time (and they may have fixed this now) you could simply do a whois "student ID" and get their basic info, class schedule, full name, address, and in some cases if the privacy function was not turned on or if you had a faculty login, you could see their SSN. I never brought this to the attention of my school's network admin because at the time I was being accused of cheating in class. I didn't want to bring more negative attention to myself. I just thought I should clear that up a bit.

El Jefe

Dear *2600:*

I just read george's article in 22:2 about the AIM Eavesdropping Hole. In it he mentions that as far as he knows this doesn't work outside of a "single external IP situation." I recently discovered that it does work with different IPs.

My roommates' computer is one that I set up and used for a while as my own before passing it along to them. During that process, I installed Trillian on it with my AIM account and a few others set up. When I passed the computer to them, I left Trillian set up for me and added a new Trillian account for them. Since I am the main account holder, when they turn on their computer it starts my Trillian account and unless they log out, my account stays on. This isn't a problem since we are almost always working together when they get on their computer and if I'm going to be sharing secrets over IM, I can always disconnect that connection (AIM gives the second account starter the option to press 1 to disconnect the first connection). As far as I've noticed though, it doesn't tell the first connection that a second line has joined.

Now to the crux of the issue. I often take my laptop on the road and sign in using the available WiFi connections. If my Trillian account is running at the same time on the other computer (back at home) I'll get the message asking if I want to disconnect the first connection. I haven't checked to see if my messages still show up, but I'd guess that they do, since I'm still getting the option to remotely disconnect the AIM connection. Now I'm curious though. Next time I'm out I'll have to check and see if there's a copy of my comments on the other computer when I return.

Ovid

Dear *2600:*

Lifetime subscriber. Reader since the TI99/4A was born. Still have one around here somewhere.... Anyhow, thank you for finally putting all the letters in one section. I know it is publishing and advertising "law" to split up articles and long sections of text to get people to flip through to the "other" pages in a publication, but I also know that most of us are reading your work from cover to cover. Sometimes multiple times. Thanks for making it easy on me. I hate using multiple book marks.

Keep up the great work. Especially, keep publishing both the deep and the simple stuff. We can't get the new folks interested by asking them to be proficient. We have to hook 'em first.

Dufu

Dear *2600:*

Just finished 22:2. Thanks for another great edition. You will probably receive many responses to Tangled Web's problems of getting the second vehicle out of the secured garage. I don't think the problem needs any major hacking. It seems like social engineering is the best way to go. Here are some ideas:

1. The simplest would have to be... play dumb. Go to the guys who run the service and say the machine won't let me out. When they say "But the computer records show that the car is out!" just say "Well there's the car. It's in. There must be something wrong with your computer. Fix it so I can get the car out." They won't be able to disprove the "computer fucked up theory" and they are probably technophobes anyway. Maybe they'll issue him a new transponder to replace his "faulty one."

2. Has he walked up to the "In" gate and tried the transponder?

3. If the gate needs a car to trigger one of those square wire in the pavement deals, he could always try using a bicycle or something like that with a reasonable amount of steel in it to engage that mechanism while activating the transponder. Otherwise he could always hang around the gate opening and use his transponder when some other car comes in.

There's probably more things he could do, but by the time he reads this his other car will be back from the shop anyway.

By the way, I was very disappointed that one of my fellow Aussies did not pick up on the April 1st dress code gag. The responses you received were very very funny.

RustyOldBoat

Dear *2600:*

This is in to response to "Tired of being followed" in 22:2. The device he describes sounds like the things I have been installing for a loan company that does high-risk loans.

In a technical sense these are not GPS systems at all because they use cellular systems for tracking. This makes full tracking like a satellite system impossible due to limitations of cellular coverage. The device manual instructs the installer to not place the antennas under metal and suggests under the dash or front or rear windows.

Once I had parked a vehicle that I had just finished under a metal carport to test the unit and see if I could get a signal from it. The result was that the unit was responding and it revealed the tower that it was near but the tracking system was unable to calculate a precise location due to the metal from the carport interfering with the antennas.

I am sure he could use some tin foil to cover the antennas to prevent being tracked.

GeekBoy

Dear *2600:*

Just dropping a quick email about the new back cover photos. They're great. An excellent way to point out the lack of foresight for some and sheer stupidity of others.

A perfect addition to an otherwise perfect zine.

MetroTek

Of course, stupidity is only one of the possible themes.

Dear *2600:*

Stankdawg, not only do I find your "owned by DDP" ad funny (referring to article "Hacking Google AdWords in 22:2) but I find the fact that in picture two the search for "google really sucks" returns 796,000 hits even funnier.

paper tiger

Dear *2600:*

I have to admit that I was quite amused reading the rants and revolts about the "new dress code" issued on April 1, 2005 for all meetings. Hackers are supposed to think outside the box last time I checked and it seems that many individuals did not realize that it was issued on April fucking First! Come on! I am sure many people have realized this but for the ones that keep complaining, become a true hacker and understand fully what is being told to you. I just started regularly reading *2600* and getting back into the hacker mode but despite the slacking off I have been doing, I need to at least open my eyes to what information is available. Thanks for the kickass mag guys!

Andrew

Dear *2600:*

I've been reading your magazine for quite some time now and have learned a lot. I'm not as savvy as most of your readers; but I'm more knowledgeable than most.

The reason for this letter is to respond to the letter in 22:2 under "Corporate Secrets." It seems that he/she works under the same conditions that I do, just on different sides of the border. The corporation I work for just installed a new system in our vehicles and threw away the old ones. The old system would ping the vehicles every 30 minutes to get a location on their whereabouts. But there was a seven minute delay; I believe, as one satellite went out of range and another one would pick back up. (I have no proof of this, just theory.) That system was defeatable, hence the reasoning for getting a new one.

The system that was written about sounds different than ours. The brains of our system is placed behind the passenger's seat with three serial connectors, two for communications and one for GPS. This is the old system again. The first method of defeating it was the old soda can over the antenna. Sort of crude but it did work. The second method is a cleaner way to do things. If it is the same type of system it downloads all of its information at night after the vehicle has stopped for a certain amount of time. You can find this out if they installed an old car phone in your vehicle. At a predetermined time the phone will dial out. After it dials out it goes to sleep until the vehicle is started again. This is when you strike. When the unit is asleep disconnect the GPS connector. You no longer have a GPS signal. You can go where you please and the position of said vehicle has not moved since you unplugged it. Do the reverse to plug it back in and make sure the system is asleep before plugging it back in. That was the old system (Highway Master).

Now we have a new system. This will interest a lot of you. This info I got straight from a tech working on the system. This system pings the vehicle every 30 seconds and never sleeps. It has its own backup battery and a tamperproof sensor. If any connectors are disconnected, it sends out a signal alerting whomever that there is a problem and the system needs checking ASAP.

The system also is a floating hot spot. That's right, it has its own WiFi transmitter, with pretty good distance on the signal. It broadcasts its SSID (@Road) and it has two IP addresses, an MIP and an SIP. I thought if I could ping the IP addresses and flood them it might mess up the system but they turned off that function for now. Oh, and it's only WEP keyed (so get cracking). This is being done to all vehicles (except management) and should be completed by the end of the year. This is being done by the second largest telecommunication company in North America.

That's all I know now. Any and all info welcomed.

MS

Dear *2600:*

George wrote in the 22:2 issue that AIM had an eavesdropping hole. When you sign on in one location then sign on at another location, it does not log off either of them. This *could* be used as an eavesdropping hole, but it's not likely. The AIM company actually did this on purpose. It's a feature that they created due to user feedback. It's not exactly a hole because when you sign on at the second location, the AIM server sends you a message that you are signed on in more than one location. If you want the other location to sign off, you just reply with a certain message to the AIM server message. The server also sends you a message if you are already on and your account logs on in a different location. It sends both locations a warning message and therefore you will not be eavesdropped upon if you do not want to be.

Shadow0049

Unless you somehow don't see that message.

Dear *2600:*

I'm writing in reference to george's article "AIM Eavesdropping Hole" in 22:2. He's correct to note that leaving yourself logged in to AIM on more than one computer leaves you vulnerable. He suggests that AIM be "fix[ed] so that, like Yahoo Messenger, you get logged out of your current session if you log in again." It's interesting to note that this was how AIM operated until about a year or two ago when they added this "feature." Never fear, however, because you can force other sessions to

close when you open a new one.

When you open a second AIM session using AOL's client or GAIM, you should receive an IM from "aolsystemmsg" informing you that you are already logged in. If you type "1" in response to this message, you will be logged out of your other sessions on other machines.

iChat (for Tiger) will prompt you to only allow one session at one time or multiple sessions. Earlier versions of iChat would receive the messages from aolsystemmsg instead.

Adium will immediately disconnect when it detects that you have opened a new session.

redjen

Dear *2600:*

First a question, then a statement. I went to your site against my better judgment (the government eyeing you and, well, you are hackers!) and was surprised to check my cookies (multiple times, as I was shocked!) and found none placed there from your site. Anywhere I have gone on the net I have a flippin' cookie placed on my computer, so how is it that it isn't necessary from your crew? Not that I don't like the idea, hell, I welcome the lack of intrusion, just totally unexpected from a hacker magazine site.

Statement to the guy who didn't like the knocking of the government and the like in the spring edition: If you don't want to hear or read about the current government being messed up, then I would suggest that you poke out your eyes and blow out your ear drums or travel to a different planet, as *anywhere* you go on *this* planet people will be saying or writing about it. As far as your judgment on "hackers," why are you filling up part of *2600* with *your propaganda* if you don't like the people in general? Save it for "Hail Bush Quarterly" as it was a waste of space and required little intelligence to figure out that you are a sheople for the government to have at their leisure.

Shadow Walker

Dear *2600:*

Why did you stop the page 33 tradition? I refuse to believe you simply "ran out of ideas." I am very disappointed in the staff for this. You have just lost a major feature in the magazine that kept me coming back every season. Fortunately enough, there are always enough other features to hold my attention. Keep up the good work.

RIP page 33 (Winter 04-05)

concerned reader

Dear *2600:*

To begin with, thank you *2600* for bringing out a *great* magazine and thanks to all the great articles that people have sent. The one article that I think was really nice in 22:2 was "Where Have All the Implants Gone?" by Estragon. I truly believe articles like that can end up changing people for their good. Again, thank you *2600* for giving people the opportunity to share!

Lews Therin

Dear *2600:*

I am writing in response to Brian Detweiler's response to "Ad-Ware: The Art of Removal." While I also did not get much out of it, it does have a place in the magazine. The magazine does try to publish some articles in each issue from easy through to advanced so that there's something for everyone. Simply going elitist and scarring away the casually interested does little for the community.

The idea that by simply saying http://www.mozilla.➥org/firefox and that's the solution is missing the point. We have to consider why spyware infects IE at the rate it does. For once this is not the evil empire's fault. Try as hard as I can I can't blame Microsoft for this issue.

It all comes down to marketing and market saturation. If you are going to write a piece of scumware then you want to target the greatest number of people. (I would say victims but the makers of this junk are still trying to claim they are legitimate business people.) The fact is that IE is on every version of Windows and has by far the biggest piece of the browser market. Again, I'd like to blame Microsoft but the fact of the matter is most users use IE because it's there and they don't know about the options.

If you're going to suggest switching to a different browser to help the issue you'd be right but you can't just say Firefox. Since the makers of this stuff are after the market share, when Firefox gets popular enough (which should be soon since almost anything you read now says use Firefox) then the scummakers will just start coding to infect Firefox.

So go ahead and get everyone to use Firefox and wait till it has the same trouble.

Also, when you suggest people use other browsers, make sure to list several others. Here's a link that can suggest many others: http://browsers.evolt.org/. Don't just be a Firefox fanboy. Realize the whole problem. We all have more to learn.

By the way, I can't help but notice Brian says "I am becoming increasingly concerned at the number of sophomoric articles appearing in *2600*" and then two letters down wrote in saying "The article quality has improved."

Witchlight

Dear *2600:*

Crash the Greenhat mentioned highlighting and writing all over his issue. I thought I was the only one to do that. Man, we are all a bunch of geeks. I think I'm going to start buying two issues too.

Proud Female Geek

Dear *2600:*

In regards to the article about AIM eavesdropping in 22:2, I am wondering if that is just an Apple thing. I remember when I was in school we had Apples and my friend showed me how if you didn't sign out of Hotmail you could go back and check someone's email. I think it was some Apple discrepancy that wouldn't have worked on a PC. It's been several years though, so sorry to say I forgot the specifics like if you needed to keep the browser window open. I am sure it could be tested though.

Also, I wanted to ask *2600* about China. My current theory is that the US is slowly losing its power and prestige and it is being transferred to other nations. Right now China seems to be getting more powerful. With your available resources that I don't have, do you think I am on the right track?

Alan

Most definitely. Only "slowly" is the wrong word.

Dear *2600:*

This letter is in response to Tangled Web's dilemma as noted in 22:2. A probable solution is as follows: Have your friend drive his/her car into the garage where your car is presently parked. Have this friend secure an entry strip card/ticket and then immediately turn around near the guard booth. Most manned parking garages will let

you leave within minutes of entry without charge and without asking you for your card/ticket since they do not have to enter a turnaround into the charge system computer.

If there is a machine at the entrance and not a manned attendant, buy two cards/tickets and scan them both upon your next entry, securing the second card for your car. Most electronic gates are opened when someone scans the card/takes a ticket and then closes after a preset time (or) when the weight is taken off the scale underneath. If this is the case, pull the vehicle off the scale, wait until the gate closes, and scan the second card. Pull through the gate this time, leaving two entries for one car (the second being for your exit).

If the attendants know you, have another friend remove your car for you with this card, or if they do not, simply drive it out yourself. Since this garage has both long-term (monthly) parking and short-term (hourly/daily) parking through the "swing-gate ticket system," it also most likely has multiple entry and exit points. Drive the car out another exit point (to circumvent any recognition by those attendants manning the garage and from cameras at that exit) separate from your friend's entry and you will be home without any problems.

Also, many garages with long-term parking have the transponder system hooked up only at the alternative/rear/special/VIP entrance and they do not have the system at other entrances/exits. If this is the case for your garage, simply bring it in the other entrance and drive out through the official exit point as if your car has been parked since your last entry without removal.

If there are any problems with the above two solutions, remove the batteries from the transponder and call the help attendant to come fix it, telling him/her it "broke" while the car was unattended. Hope this helps!

By the way, others will be interested in knowing about an e-book I stumbled upon regarding the circumvention of the American banking and tax systems through offshore tax avoidance methodology, many using digital approaches at http://www.lulu.com/content/69514.

2600 is an excellent mag and always an informative read. Keep up the excellent work!

GulfstreamXo

Dear *2600:*

I have been reading your mag for at least ten years. I don't always agree with your views but we agree more than we disagree. The information is the important part. I have a couple of comments.

First is about Estragon's rave on implants ("Where Have All the Implants Gone?" 22:2). I believe he is naive to not see the answers in his own writing. Money is the "power that be." Whoever controls financing the ventures he talks about doesn't see the return on the investment. I really do not see as many people as he imagines wanting an electronic chip stuck in their body. I suffer from carpal tunnel, literally, and it is painful but you could not pay me to have an implant. And I know which half of the intelligence scale I am on. He should look more at a classic bell curve and find himself in a larger group.

No implants because there is not enough money in it. They would rather make a dollar apiece off 50 million people than make 50 dollars off a couple of thousand.

Second, about "Tired of being followed" in the same issue, my advice is to "shut the hell up and go to work!" Being watched sucks. I am working now under constant camera surveillance. I have been for four years. I am being watched on live camera and recorded as I am writing this. If you do your job and they cannot see it, who the hell wants to work for them? How much is the equipment you control worth? I operate a $500K machine, making $5K to $25K per piece parts and have a toolbox worth about $3K! I worked for a company with funky security and they were robbed of every employee toolbox in the place and some of the company tools as well. Ask those people about cameras.

If I owned the company and found out you screwed with the system, you would be out of work. I would want proof but when and if I could prove it, you would be gone. I know for sure there is a policy at every place I have worked at that employment is "at will." Meaning I am employed at their pleasure. There does not have to be an explanation, except you're fired. Almost all employees are supervised. What makes you special? Go to work and shut up.

Metal Cutter

There's a big difference between being supervised and having your every movement scrutinized. Why is it so necessary to treat your own employees with such suspicion? If you keep getting screwed by them, you're either extremely bad at hiring decent people or you're doing something to piss them off. Most people we know who are under constant surveillance and forced to submit to drug and lie detector tests don't think of their employer in the most flattering of terms. And in the end that will lead to the termination of the employer.

Dear *2600:*

This is referring to a past issue where a person said that deepfreeze can be disabled by booting with a 9x boot disk. An easy fix for this is to change the boot order so it goes to the hard drive first, then password protect the bios. We did this all the time at my last job. Resetting the bios is easy. You just need to pull out the battery but if you're going to do all that to get access to the drive you may as well just pull out the drive, take it home, and make it a slave on your system.

pyroburner69

Advice

Dear *2600:*

I've read many letters that people have sent to you saying that they hide their issue of *2600* or read it in private so that they won't attract the "wrong" attention, receive weird looks, or for fear of being punished in some form, be it expulsion from work, school, or something similar. My response to these people is *be proud of who you are!* Isn't this the type of reaction (weird looks, punishment for reading and educating ourselves, etc.) we are trying to abolish in the first place? How can we do so if we hide what we learn and who we are? Some of you may be thinking "Who's this guy to tell us not to fear these reactions and punishment?" Well, let me give you a little background on myself. I've been an avid follower of techno music since I was ten years old and the rave scene since I was 15. I'm 24 now. Throughout this time I was always looked down upon and judged because of the "popular" belief of what a raver is supposed to be: an uneducated party kid who takes lots of drugs. Of course this is just a stereotype. I didn't let this *opinion* pull me down and stop me from listening to the music that I loved or dressing the way I liked. Once people moved beyond their stereotypical beliefs and got to know me, they realized that I wasn't some "druggie party kid" but that I was educated, talented, and a "likable" person.

When I started getting into computers and read my first *2600* six years ago I knew that the hacker/phreaker mentality was something that I would support just as much as the electronic music scene. I never hide my copy of *2600* or close windows of hacker sites on my PC just because someone is watching or giving me a "weird" look. I just explain to these people what it is I'm reading and why. I tell them that I'm not a criminal learning about computers to steal identities or money from their bank accounts. I explain to them that hackers and phreakers educate themselves on everything having to do with computers/phones because we are interested in knowing how they work, how these systems' problems can be fixed, and how they can be made better. *You guys should do this too.* People are only fearful and judgmental of that which they don't understand. Break these people of their ignorance by being patient and educating them on what the hacker/phreaker community is really about. This is the first step to defeating the media stereotype.

s00p3r sKri8s

Dear *2600:*

Ever thought of carrying golf shirts in your store (also called "polo" shirts or just "collared" shirts, depending on which part of the nation you're from)? I bet a lot of readers work in the corporate world where t-shirts are a little below the implied dress code, but golf shirts are all the rage. All you need is something clever but not particularly offensive on the chest.

I'd also like to request your next line of apparel, whatever it may be, come in a color other than black. Almost everyone at HOPE wore black t-shirts. Encourage some diversity in hacker clothing!

A Big Corporate Tool

Thanks for the ideas. We're always open to suggestion on styles, colors, etc.

Help Needed

Dear *2600:*

I read your magazine every time I am in the USA. I really enjoyed your article on war driving with a Pocket PC.

I know this sounds a bit unconventional, but I am actually looking for a hacker specializing in bluetooth viruses for an art project for my next art exhibition. I am a mobile artist and I speak about how data moves (it's fascinating to me). I tie it all back into the ancient texts of the Vedas and Sutras, the first people to talk about energy and how to use it (it's a long discussion).

I would like to build a non-harmful bluetooth virus that propagates itself via all bluetooth channels like the Caribe virus, however it wouldn't harm the cell phone device in any way. I would like it however to deposit a graphic file in the gallery with a sign saying "you've been bitten by the mini me virus, please see xxx url for more information." Then the bluetooth virus would push itself via that phone's channel to other bluetooth devices (not as annoyingly as the Caribe because that just blocks your phone and I don't want to be too annoying - I just want to track how and where the data goes). The person then goes to the site where they see a map and are asked to type in their geographic location when they got the virus which will then be plotted on the map. In this way I can start to understand in a more graphical manner the bluetooth channel. In my exhibition I would like to have a big plasma screen where people can watch the movement of the graphic. Of course this will be well advertised and alerted, so as not to cause a panic in the world.

Do you have any clue where I could find a person who would perhaps be interested in building such a virus for me? It is very important to me that it be a trusted individual, because if they were to make it a harmful virus, it would really destroy the faith in bluetooth, etc. I would like to understand viral travel so that it can be exploited in, say, marketing channels, or the technology then sold for viral advertising campaigns. So the person who makes it with me can profit. If you can see any other benefits that I could offer the hacker, please let me know.

anina

We somehow doubt the people infected by this virus would find it any less annoying than if it were indeed harmful. And unless you plan on getting the word out on billboards around the planet, it's quite likely most people wouldn't know it was harmless. While the results would indeed be interesting, the execution is flawed at best. And the idea of using this sort of approach for advertising is even more repellent.

Dear *2600:*

I was reading your meeting requirements and I came across your IRC channel. I thought I would check it out. Now I don't know if it's because I am new to IRC but when I typed your address in and connected I got this in return:

"Closing Link: [myhostname] (Invalid username [_WiseCrack])"

Now I'm not sure if there is a password or something or if I can't use WiseCracker as my username, but if I could get some help as to why I get the error that would be great.

WiseCracker

We suspect it's because you have an underscore as the leading character in your nickname. That sort of thing does tend to cause problems with many IRC servers and clients. For those unfamiliar, our IRC network is run at irc.2600.net (port 6667) and the general channel for 2600-type things is #2600. You can also participate in your own regional 2600 channels with the format of #xx2600 inside the United States where xx is the two letter state code (#ca2600 would be the channel for California) and #2600yy outside the United States where yy is the two letter country code (#2600ca would be the channel for Canada). You can also start any channel you please, 2600 or non-2600-related.

Dear *2600:*

I have read your magazine for a few years now and truly admire the breadth and depth of articles and topics! I also admire all those very smart people who contribute to the magazine. It is those smart people who I am asking for help from now. Let me explain the situation:

I have recently placed an ad on the petfinder.com website trying to find a new home for my cat. I would have never surrendered my little cat, but she has herpes and my boyfriend's cat is in very poor health such that if he gets herpes he will likely die. And I am moving into our new house with my boyfriend in October, as I am five months pregnant now. My cat is a wonderful little orange thing and I really hope I can find somebody who would love her as much as I do. But this letter is not about that.

I have received three responses to my ad that disturbed and scared me a lot. There are many strange things about those emails, the most disturbing ones are:

1) It was the same email (pretty much, even a poem at the end was the same!) written in very bad English, but signed by different names and sent from different email addresses;

2) The author was urging me to contact a pet moving company's email, even without talking to me on the phone or seeing my cat's pictures;

3) All emails were sent from the same IP subnet, which, in my opinion, indicates that they were all originated from the same organization;

4) In all emails, the author was referring to him/herself as Mr./Mrs. FirstName (for example Mrs. Doris), whereas no normal person would do that. You either use the Mr./Mrs. LastName or Mr./Mrs. FirstName LastName format.

There are other things I did not like about those emails but I think it would be better to just forward them to you.

I am very worried that this is some kind of scam where people are trying to collect animals for some horrible purposes. Needless to say I would never give my pet to them but I am afraid other people might not be so careful. I cannot even think of what would happen to those poor animals.

I would really like to try to track down those emails and find out who is behind this scam. It is not easy though, and I'm afraid I don't have enough expertise in this technological area (even though I am a software engineer myself). So I thought that maybe some of the bright people writing for your magazine who know how to do this stuff could help me. I would really appreciate that! I think the goal is very noble.

Meanwhile, I really worry about other people and their precious pets falling victims to this scam. I sent an email to petfinder.com asking them to post some warning message, or something like that to ask people to be more careful.

Marina

Not surprisingly, this identical letter has been seen before in similar circumstances. We're not convinced it is necessarily targeting animals however. Since at one point in the email, the possibility of doing a bank transfer to pay for your pet is mentioned, it's very possible that it's all just a scam to get your bank info. Regardless of what it turns out to be, we're certain that it's a scam of some sort. We call on our readers to help figure this one out so we can spread the word.

Dept. of Injustice

Dear *2600:*

As a longtime reader and writer, I should have probably listened to all the negative comments I've heard regarding the American train system, in particular, Metro North Railroad. As I'm sure many readers are aware, Metro North now relies solely on TVMs (Ticket Vending Machines) to manage all transactions. Gone are the days of talking to a human being; we're now forced to deal with a rather confusing machine whose screen was in no way made for bright, sunny days.

Recently I was making a trip from my hometown to Bridgeport, Connecticut, a short trip that should have cost only $1.50. My friend and I had a boat to catch in Bridgeport and we arrived at the train station with plenty of time to spare. Lo and behold, a woman was having trouble with one of the ticket machines. Another person helped her, but apparently couldn't figure out the problem. They moved aside allowing me to step up. Sure enough, I had the same experience. You would press "B" for Bridgeport and the machine brought up Ansonia. A simple coding glitch, to be sure; hey, they happen, and aren't usually a big deal. The problem was, by the time it was realized it wasn't human error, the train was pulling up. We couldn't miss the train, so we hopped on and explained to the conductor what happened. I told him I was more than happy to pay the $1.50.

No go. The cost of the ticket was now $7, and he insisted that was what he had to charge me. Don't get me wrong, I understand this man was just doing his job and in no way responsible. I paid the $7 and called customer service when I got home. According to them, if at least one machine is working then I'm SOL and should not expect a refund. The customer service woman was very nice and sympathetic, but bottom line, there was nothing they could do.

Why must I be penalized for Metro North's computer glitch? I had tried to get my ticket, done everything I was supposed to do, and ultimately had to pay the price (and then some). Yes, I'll admit, it's a matter of a few bucks. But think of all the revenue Metro North must make from these kinds of things. For the record, I will happily pay the fee of $1.50 to occupy a seat from my town to Bridgeport, but I will continue to insist upon a refund of the balance.

Screamer Chaotix

Please don't let this one go. What Metro North did was atrocious and it's time they learned that the public isn't going to stand for it. You are not obligated to troubleshoot their machines and hop all over the place until you find the one that works. You made the attempt and presumably the problem can be documented (unless they're so corrupt that they've engaged in a coverup). Write a letter to the head of the MTA, to your local newspapers, and even contact your elected officials. It may only be a few dollars but the resulting publicity will cause them to rethink the next time they try and rip someone off. It will also inspire others to fight back next time something like this happens to them, whether it's Metro North or someone else. Good luck.

Dear *2600:*

In response to Public Display's letter about his school password/username system in 22:1 in the Utter Stupidity section, I have had the same dilemma. In my school your user ID is your graduating year and then four random numbers. Graduate in 2008, 83456. Now the passwords are something random: tree, date, note, paper, etc. But all the admin accounts, which you can find by going into the security option of the C: drive, are simply just username and password the same, like SA and SA. Now, my friend and I found this out. When you are on the account, you have access to grades, principal/teacher files, student files, and so on.

All my friend and I did was look around and then we left a .txt file in the tech guy's folder which said "Hey, found a hole in your system, here's how to fix it, etc." When they found that, they traced it back and we were given ten days out of school suspension and banned from further computer access as long as we are in the school's district.

Now I think that's a little extreme, don't you?

fallen

It's extremely stupid and indicative of administrators who have no control over their systems and punish the first person who tells them this as if they were the ones responsible for their own ineptitude. As they have already unfairly prosecuted you, we suggest letting everyone in the area know the specifics of the case until they're shamed into apologizing for their irrational reaction.

Dear *2600:*

Keep up the great work guys! This is what I got back when I submitted your site for approval from our work's filtering service.

"Thank you for submitting a web site unblock request to our Filter Review Team! This website is blocked because it contains information regarding militias, illegal weapons, bomb making, terrorism and similar sites. Please review our filtering criteria located in the support section of our webpage.

Thanks again for your feedback.

Filter Review Committee

Site: http://www.2600.com/"

pukethecat

And we hear that the people who run bsafeonline.com are a bunch of child molesters. See? We can accuse people of things too.

Dear 2600:

About six years ago when I was in seventh grade, I had just started looking into computer security. When using a workstation in the school's brand new computer lab, I noticed that there was a lot of filtering going on and a lot of access restrictions. I started wondering how this was being done and how easy it would be to defeat.

I found out that the computers (Windows 98) were running the Fortress 101 security software. I did a web search on how to defeat it and found a good list of vulnerabilities. I went in and changed the home page in Internet Explorer to this website. Mind you, I didn't have to do anything to change this. The Internet Explorer preferences were unprotected. I didn't change a single thing on this system.

About a week later I received a hall pass in the middle of English class. I went to the administration office and discovered I was meeting with the school principal and the school's "tech guy." I was informed that what I did was "illegal" and that I was going to be suspended for five days, lose my computer privileges for the remainder of the year, and that I was lucky I wasn't being expelled. After my suspension was over and I was trying to get through the school year, on multiple occasions the school's "tech guy" (who was about 40 years of age) taunted me whenever he passed by me in the hallways - things like "Look at me! I'm a hacker" and other comments in the same context.

I find that this is a showing of mass paranoia of "hackers" and computers in general. People who aren't knowledgeable in the world of computing shouldn't have the authority to legally (or the equivalent) act upon actions that they aren't qualified to understand. I have seen in the past six years that things have gotten a lot better (except for the time I was yelled at for changing a setting on a computer monitor in high school).

Luke

In some places things have gotten better. In others they've gotten much worse.

Dear *2600:*

I am sure you have heard of what is happening to the Kutztown 13 (www.cutusabreak.org). What is *2600's* take on this issue? Do you think what ensues will set a precedent? What would you consider an adequate punishment for these students (as they did break their ToS)?

David

This case involves students in Kutztown, Pennsylvania gaining administrative access on laptops distributed by the school district due to incredibly bad security (like having the passwords written on the back of each computer). Thirteen of these students were then threatened with felony charges. Thanks to a well designed and publicized website and a good amount of public outrage, we're happy to report at press time that this is no longer a threat and that 15 hours of community service is the penalty that was imposed in the end. There's a big difference between breaking Terms of Service and having no security at all which was the case here. That's why we think that even this is an overreaction. The school district hopefully learned a lesson here but we wouldn't be surprised if they didn't.

Memories

Dear *2600:*

Reading through the back issues for 1984 and 1985 over the last couple of days makes me sad. I didn't know you existed until a couple of years ago. Not that I was ever into phreaking, except to listen in to an international conference courtesy of a friend. But hacking? I was probably one of the earliest hackers around.

I started with computers in the late 60s on IBM mainframes and by the early 70s I was a systems engineer. That was fun! My first major job was to write a language so two Honeywell computers (mainframe and mini) could interchange data. I also had to debug new hardware on the systems. (The first cassette tape installed in Australia is one of my fondest memories of those times. I had to get into the hardware in a big way via software - I am not into the hardware side.) Went on to VAX and various others until the PC came out. What a fun world that was!

I used assembler or machine code and they were powerful (forerunners of C, of course, but in my opinion better than C). I moved into security for a while and seemed to do pretty well there. Creating systems I couldn't crack was great - and no one else cracked them either. However that led me inevitably into trying to crack other security systems - innocently at first, just to get the idea of what sort of security was around. Got into a few interesting systems - interesting because (a) I wasn't supposed to be there, and (b) their security was allegedly pretty inviolable. Ha!

By the early 80s I was using UNIX at a university and was on the net. Suddenly the world opened up. We had access to virtually every X-Net on the system - as long as you could get into them. I didn't seem to have much trouble with that either. Then Big Blue went ballistic and brought out specs on their about-to-be-released PCs so software writers could have the opportunity to write for them before release and BB would have masses of software to offer along with the hardware. Not much was left to the imagination!

PCs were fun. Using 8086/8088 assembler got you into anything! Which is what prompted this lengthy ramble. In 1985 you people were bemoaning the difficulty of getting enough info about PCs as there were so many different ones by then. Believe me, they weren't so different that one couldn't swap between them quite readily, as long as you stuck to assembler and used Debug.

I am now retired and haven't bothered to try to crack Windoze - too lazy. Hate it with a passion, too, which probably adds to my indifference. All the stupid little wannabes with their Tinker Toy viruses, and the damn fools who steal credit card numbers and IDs have really put me off. To me a hacker is one who gets into a system for fun, maybe looks around a bit and plays with it, but

does no damage and hurts no one. Anyone else is not my kind of person.

Thanks for tolerating this long and unnecessary bit of trivia, which will enlighten no one, but the urge to tell someone of some of the things I used to do was overwhelming. I've never admitted to illegal entry into machines before. I know you guys would understand, even if you aren't interested.

Love *2600* and am almost tempted to get back into a bit of good clean fun.

Mudwasp
Sydney, Australia

It was great hearing these recollections. Thanks for sharing them.

Dear *2600:*

As an employee (outside tech) for Verizon, Bell Atlantic, NYNEX, New York Telephone - well let's just call it "The Company" as my contract read for 25 years, I couldn't agree with you more. The Company has turned from a Mom and Pop take care of employees and customers corporation into a "how's the stock doing electronic conglomerate" caring only about the bottom line and the Golden Parachutes of their hierarchy. It used to be a great caring place to work at and for the customer to deal with. It was a company that cared about customer service or employees' health care and rights.

Well, we could blame it all on Judge Greene and divestiture but it goes a lot further then that, you can be sure. Before "The Split" all The Company's top lawyers sat down and figured why fight it. It would be to upper management's benefit to allow the termination of this great company. They saw dollar signs and went down easy knowing what was going to happen in the future. You don't hear much of MCI and Sprint like you used to. Wait and see, they will be a memory before long. With FTTP (fiber to the premises), Verizon (The Company) will be the monopoly once again in everyone's home and computer, knowing exactly what shows you watch, what products you use... well, you get the picture I'm sure. Who is worse? The feds or Verizon? You got me. Customer service is a contradiction in terms The Company doesn't care about the customer or the employee (the old backbone of the company). The employee in return cares nothing about The Company or the customer. All I can say is good luck when your line goes out again. I hope it's not me fixing it because as the old adage goes "what goes around comes around."

CWA1108

Reestablishing Contact

Dear *2600:*

First, I would like to say that I think your magazine is great. However, I have only had two occasions to read it. When I lived in Washington State about eight years ago, I had a neighbor who was pretty smart with computers. At the time he and I were into the same things in computers, but he was always on a power trip. Whenever we played with super soakers in the summer, he had to have the most powerful one. If he didn't and someone else did, that someone wasn't allowed to play unless they gave their super soaker to him. Being that he was four years older than me, I never could really stand up to him without repercussions. Anyway, one of his power trips was keeping an issue of *2600* away from me. I was at his house and had discovered it. When he caught me reading it, he snatched it away and told me that it was for "eyes only" and I wasn't allowed to read it. I didn't think much of it, except that it was just another control thing for him. Because I didn't catch the name of the magazine (I was busy reading the articles, not looking at the cover), I could never remember the name of it. Over the last eight years I have gone through spurts of trying to find the magazine with no success (as I could not remember the name). I finally gave up about two years ago because I just figured that it was probably a local magazine for the state of Washington (I live in New York now).

Then a few days ago I was browsing the magazine racks at Barnes and Noble, looking for a Linux magazine that had the Fedora Core 4 distro. Then I saw the little magazine and instantly knew what it was. I picked it up and am about to subscribe to it right now. God, how I hate that kid who didn't let me start reading it eight years ago. Think of all the information I have missed! Damn bullies!

Woodstock

We're sorry one of our readers treated you this way. We usually attract a better class of clientele.

Dear *2600:*

I just want to *thank* you for sending me the renewal notice. I did not realize that I had already received my last issue. I just wanted to let you know that I thought that was cool of you to remind me. I love the magazine, I will replace my H2K2 shirt someday (three years and still looking good), and the *Freedom Downtime* video is very cool!

CD

Don't count on that H2K2 shirt being in stock as the conference was three years ago. We're glad you enjoyed our renewal threat letter and acted upon it. Among other things it saves us a visit.

Dear *2600:*

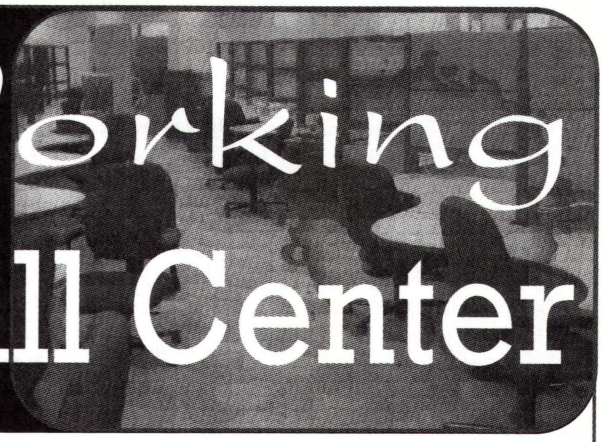
I haven't picked up your magazine since last year. I just haven't been near the store to pick one up unfortunately. *Spam* finally came in handy! I got an email today for Viagra (big surprise eh?). Anyway, the address was from lorie@2600.com. Having been an avid reader I thought you guys were emailing me asking me where I've been lately! Since I buy the magazines off the rack, I said to myself... damn these guys are good! How'd they track me down? But alas, just another one of many Viagra sales. Anyway, at least it piqued my interest again and I plan on heading out tomorrow to get the latest issue. It has always been a good read for me.

jay
Norton, MA

This is the first - and probably the last - time that spam has ever served us. By the way, we trust that anyone who sees such email knows that it has absolutely nothing at all to do with us and that the headers are completely forged. But if you do get one of these, please give us a kind thought nonetheless. That'll show those spammers.

Got a letter for us? Send it on the net to letters@2600.com or use snail mail: 2600 Letters, PO Box 99, Middle Island, NY 11953 USA.

Not Working at a Call Center



by XlogicX
XlogicX@phx2600.com

Back when I was in high school I worked at a call center, a job many of us have came across. I've done a variety of call center jobs: inbound credit card activation, outbound telemarketing (didn't last very long), and outbound surveys. Right now I'm back to the call center after years working as a rent-a-cop. I now do tech-support, and I'm reminded of a trick that still works: How to not work a whole shift by using the phone system.

Discovery

It all started back at the original call center while working with some friends. We had a 30-minute lunch and two normal ten-minute breaks. We also had an extra ten minutes of break that could be used however we wanted. We could take three three-minute 20-second breaks or five two-minute breaks. My good friend noticed a timing pattern in the queue we got after taking a break.

Say we had a 15-minute wait between calls normally. After taking a break, we would be waiting on the phone for just about 15 minutes until we got a call. My friend looked over the supervisor's monitor and saw that after logging back into the phone, that user would be placed at the bottom of the queue. This doesn't sound like too big of a deal; most people know that this type of system works this way. It's only fair that the agent isn't bombarded with calls right after break. But that's not how the mind of a hacker thinks. How could this be used in a way it's not intended to be used?

The Exploit

It's the extra ten minutes. Knowing that there was a 15-minute wait period, my friend would wait ten minutes and take a one-second break. Fifteen minutes after the break, he got a call. To recap, that is 25 minutes between calls. After trying this, he took a one-second break every ten minutes for the remainder of the shift. For that entire period of time, he mysteriously didn't get any more calls. He told us of his discovery the next day. So for our entire shift, none of us took a single call - for a whole eight-hour shift!

On most call center phone systems, this is an "aux" code. There are different aux codes for different reasons: lunch, training, data entry, break, etc. For this exploit, we used the aux code for a break (Aux #2 where I work now, on an AVAYA phone system). It was OK at the original call center because nobody paid any attention to the logs for break as long as we weren't exceeding our ten-minute limit to our extra break time. You may not want to try the method that lets you not take any calls, but there is another way to reduce calls that probably won't get you caught, though it won't give you as much free time as the above method. Say you notice there are about 16 minutes in between calls and you are about ready to go on a break or lunch. Most people wait until they finish a call and then take a break. In our case, wait 15 minutes (or as close as you can without actually getting the call) after your last call, and then go on break. Those are 15 whole minutes of easy money, and you'll probably end up doing this four times in a shift. So that can add up to about an extra hour of no work in each eight-hour shift!

Conclusion

Turns out this same old trick works at the call center I just started at. I'm not going to be using it anymore though; this place audits a lot more. It wouldn't have been a big deal to lose my job in high school, but now that it gets me food and a place to sleep I don't want to mess around as much at work. I still may end up using the trick of waiting after a call before lunch though as this is less noticeable. By the way, I did end up getting fired from that original job while I was in high school. I guess putting a hard drive magnet up to a non-degaussable monitor wasn't the right thing to do, especially when the monitor was in the cube next to me with someone using it at the time. They said they would call me back if they needed further help. It's been a while.

Shouts: Evin, Skyler, Dual_Parallel.

Securing Your Wireless Network

by Seal

The purpose of Local Area Networks (LANs) is to facilitate the sharing of data between multiple computers. Because of their disposition, computers within the LAN treat each other differently than they do those on the Internet. It is that distinction which leaves them vulnerable to certain attacks, such as ARP Poisoning. Windows users are even more vulnerable; installing a keylogger across a network takes only a matter of seconds on computers with default settings.

The lack of physical access was the principle means of protection with wired LANs. With the advent of wireless routers, however, that is no longer the case. WEP (Wireless Equivalency Protocol) is the traditional system of encryption to protect wireless communications. Without it, an intruder can easily sniff out sensitive information sent over the airwaves. Unfortunately, WEP is flawed and can now be cracked in a matter of minutes. It has become obsolete and virtually useless as a means of protection against malicious users.

There are a few options to protect oneself. You can upgrade to a router supporting WPA or VPN, both providing more reliable forms of encryption. However, this option costs a fair bit of money and there's always the potential that the protection algorithm will be cracked in the future. There is another option however: bypassing the router entirely and using SSH tunnelling to encrypt our data.

This means that if someone were to intercept the wifi signals, they would first have to crack SSH in order to see its contents. There are two advantages to this method: the encryption is already strong, and because the solution is software and open-source based (i.e., not reliant on the router), patches could be issued to fix any potential vulnerabilities within the encryption.

The execution of this system necessitates that one computer be connected to the router via ethernet. This tends to already be the case with most setups. That wired computer will also have to run an SSH server. Linux users: that's already done. For Windows users, I recommend that you download *free* Cygwin (see below for URL) and opt to install the OpenSSH package during the installation. Once that's done, start up Cygwin and type in "net start sshd". From that point on, the server will launch with Windows. Type in "net stop sshd" to stop the server.

We aren't finished with our server, however. We must then install a proxy server onto the machine. Windows users, I recommend you download a *free* program called "Proxy" from AnalogX (see below for URL). Install it, and choose what communications you want it to handle and thus have secured (i.e., HTTP, FTP, etc.). At this stage, the setup is complete. We must now configure our clients (aka wireless computers). Linux users, I recommend you try "Squid" as the proxy server.

The next stop is to tunnel through sensitive communications. Windows users, I recommend that you use the *free* Putty (see below for URL). Now you want to forward the information. To do so with Putty, in the options select the "Tunnel" category (it's under the Connection --> SSH banners). In source port, put in "80" (for web traffic), write "localhost" as the destination, and select the "local" box. If you're using AnalogX's proxy, write in "localhost:6588" as the destination. The destination will vary if you're using another type of proxy server. Press "Add". Repeat adding ports for what you want to secure, using the following table for reference:

Protocol, Source Port, Destination
Web Traffic, 80, localhost:6588 [for those using ➥AnalogX Proxy]
E-Mail (Incoming), 110, localhost:110
E-Mail (Outgoing), 25, localhost:25
FTP, 21,localhost:21
Newsgroups, 119, localhost:119

In the "Session" category, write in the internal IP address for your server. If you don't know what it is, on the server computer go into CMD (Run --> Type in "CMD") and write "ipconfig". It will then display its IP. Once you're done, click on "Open" with Putty to connect to the server. When it asks you for credentials, enter the username ➥/password needed to log on to Windows for that machine. All your web, mail, etc. information will now be highly encrypted.

Finally, we have to tell our programs that are transferring the data to use the proxies. You will want your proxies to be specified as "localhost"

(aka. 127.0.0.1). So for example, in Firefox [Multiplatform Internet Browser] you will want to go into Tools --> Options, and click the "Connection Settings". In the dialog window that appears, you will want to put in "localhost" as the HTTP proxy and write in "80" as the port. The settings for the SSL proxy are the same as that for the HTTP.

Badabing, badaboom, you're done! Now this was pretty much a one time process. Assuming you saved your SSH client (i.e., Putty) configuration, the only thing you have to do next time you reboot that wireless computer of yours is to reconnect via SSH to your server.

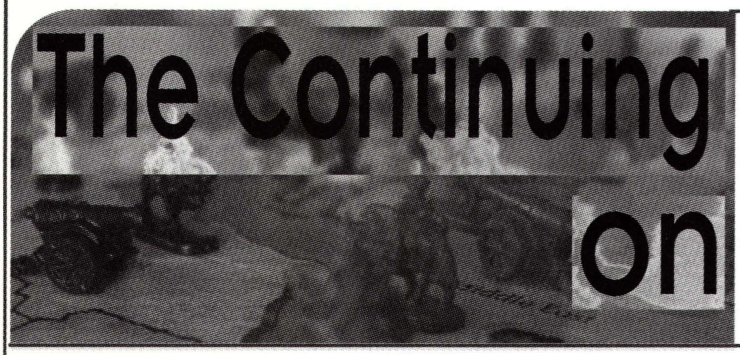
Enjoy your wireless and *secure* Internet experience!

The possibilities don't end with the borders of your wireless access point. Let's say that you're in a cafe with open wifi. Why jeopardize your information when you can tunnel via SSH to your server at home and rest assured that your information is virtually impregnable?

Why must the server be connected via ethernet? If it wasn't, then despite the fact that our wireless computers would send information to it encrypted via SSH, the server computer would itself send information with at most WEP to the router. Defeating the purpose of this exercise.

Resources

Cygwin: http://www.cygwin.com
Putty: http://www.chiark.greenend.org.
➥uk/~sgtatham/putty/
AnalogX Proxy: http://www.analogx.com/
➥contents/download/network/proxy.htm
Squid: http://www.squid-cache.org/



The Continuing War on Spyware

by Inglix the Mad

As a full-time student and PC technician for a mid-sized PC company I read Patrick Madigan's article with interest. It was an excellent primer on Spyware detection and removal tools. The state of today however, given the possible lag time in the article, dictates a much different approach. Mind the fact that if you are unable to repair a system within two hours, you are probably better off backing up your data then reloading. The previous article and this one should help you arrive at a point where you can at least perform a backup of your vital data.

First let's touch upon a couple of tools Mr. Madigan did not reveal. The first is Security Task Manager (http://www.neuber.com) which allows one to kill many running processes and toss them directly into quarantine. The best part of all is that it includes a couple of niceties such as listing who made the file, and event gives the "readable" text contained within it. This excellent tool has one last feature, the ability to "Google" the process that first takes you to the Neuber Software page which lists anything other users of the software have posted. If it is not listed or you're just not sure whether or not to believe it, you can continue onto Google to check what is linked on the process.

Second is a tool called LSPfix (http://www.➥cexx.org). This tool lists all of the LSPs (Layered Service Providers) in a system and allows you to remove them. While one cannot say enough good things about this tool it is, as Security Task Manager also is, very dangerous. Using these tools without taking precautions can render your system unusable and possibly unrecoverable, so take advantage of the third tool.

The third tool is Google itself. The collective power of the Internet means that people help each other on a regular basis and many Spyware files are identified in a quick manner. Beware though, for I have seen a few sites that purport to help remove Spyware while actually causing you to either download more Spyware or making your tools ineffective.

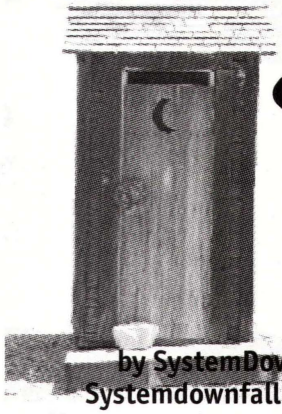
There is one more tool and it is the most important: your own mind. Over the past few months, Spyware authors have become increasingly sneaky about hiding their files, not naming the files and directories they hide in properly. Since they are dumping them in various places around the hard disk, here are a few common places: Windows, System (for Win9x), System32 (2k/XP), Common Files (under Program Files), My Documents, the Temp and Temporary Internet directories, and of course the root directory. Now to find many of these files you will have to enable showing hidden files, extensions for known

file types, and the protected operating system files. You may find these options through /Folder Options/View.

Now as for identifying Spyware files, look for small files with recent creation dates. Check to see who the company is that created the file, and for heaven's sake don't delete it if it says Microsoft Corporation. Look for files with odd names that are similar, but not identical to real system files (i.e., Kerne132.dll instead of Kernel32.dll - that "1" instead of an "L" is pretty tricky to the average person) or ones that have total garbage names like wwlkjfo.exe in the above directories. Right-Click on the file, choose Properties, and see what info is available.

Finally, a word to be wary for the future. Rootkit attacks are coming, if not already here. Microsoft themselves (http://research.microsoft.com/research/pubs/view.aspx?type=Technical%20Report&id=775) has published an article on them. They have released a beta removal tool but even they admit that the only way to be positive a rootkit is gone is to format and reload your computer. I think I may have found a couple of these myself by accident. These files that I had to delete in either Safe Mode, or even more drastically in Safe Mode Command Prompt, deny any other attempt to remove them.

I've gotten quite good at removing Spyware over the last year. It is the number one problem for all computer builders. Being at such a company that is not huge, I can only imagine the nightmare for those smaller than us, much less the end user. I urge everyone to protect themselves by using a smaller market share browser, avoid the MS email client, and get smart about downloading "free" programs. Donate money to the major Spyware hunters - they help protect you. Finally, never, ever, under any circumstances, click anywhere on a pop-up.



Hacking Image Shack

by SystemDownfall and Worm
Systemdownfall@blueoxidine.com

Many people use Image Shack (imageshack.us) to quickly host a picture to show to their friends or to throw a screenshot on for some people to help with tech support or whatever. But one thing that many people forget about posting personal images on imageshack is that they *are not* private. Anyone who goes around typing in random numbers can find that image. Let's start by looking at the layout of the url we will be using. When you upload a picture to imageshack it gives you about four different choices of URLs to use. We have chosen to use this one because it is the easiest to guess since the other ones add other random numbers to them: http://imgXXX.imageshack.us/my.php?image=XXX.jpg. The first set of Xs is the server number. All servers start with "img" and end with between one and three numbers. An example of a server number would be: "img216." The second set of Xs is the image number. Images can have names as well but it is easier to guess the numbers. Numbers can also be as many numbers as the person wants but the most common number of digits is three. The easiest way to start doing this is to just type in the url http://imgXXX.imageshack.us/my.php?image=001.jpg and move up in numbers until you find something interesting. Believe me, I have found things that are *very* interesting. After doing this for a long time, we decided we needed a better solution: a script! So we wrote a perl script that parses through the html and downloads the photo to the current directory, then moves on to the next image. Here is the script:

```
#!/usr/bin/perl -w
use strict;
use WWW::Mechanize;
use WWW::Mechanize::Link;

#Create an Object
my $mech = WWW::Mechanize->new();

my $number;

foreach $number ("000" .. "999") {
#Url to search images on.
my $url = "http://img216.imageshack.us
➥/my.php?image=$number.jpg";

#Request webpage
$mech->get( $url );

#Search for all links containing .jpg or
➥.jpeg extensions
#in the url.
#Everything in between qr/ / is what to
➥search for
```

```
#The . means any character usually but
➥we use \. to escape it
# and make it literal. Then we did
➥(jpe?g) which means to search for
#the text jpg or jpeg.
# The $ character means the end of the
➥line/string.
# The i at the end means make everything
➥case insensitive

my @link = $mech->find_all_links(
tag => "a", url_regex => qr/\.(jpe?g)$/i);


my $lurl;
#find_all_links returns a link object
# and in order to get the url from the
➥object
# you have to do a $link->url.

foreach my $currentlink (@link) {
 $mech->get( $currentlink);
 $lurl = $currentlink->url();
}
#Take done.php?l=img301 out of the URL
➥and replace with img301/
$lurl =~ s/done\.php\?l\=img216\//img216
➥\//;

#Save image to file
$mech->get( $lurl, ":content_file" =>
➥"$number.jpg");
}
```

It works very quickly and you get a lot of good stuff. The best idea in my opinion is to set up a web server and make a directory within it to run the script. Then you can access your new picture database from anywhere! Now, this script only finds jpg or jpeg files and only on one server. You would have to edit the server number to do it on a new one. This script also requires a few perl modules which can be downloaded at www.cpan.org. Here is a list of all of the modules needed: HTML::Form 1.038, HTML::HeadParser, HTML::TokeParser 2.28, HTTP::Daemon 0, HTTP::Request 1.3, HTTP::Status LWP 5.76, LWP::UserAgent 2.024, URI 1.25, URI::URL, URI::file, and WWW::Mechanize.

I Am Not a Hacker

by mirrorshades

The media tells you that "hackers" are either unsupervised teenagers who break into computer systems and steal credit card numbers to use at pornographic websites, or scum-of-the-earth anarchist rebels who write viruses designed to destroy ATM networks and shut down the "evil corporate system."

The truth is that "hacker," as a title, is dead. The title conveys an eclectic sense of rugged nobility from a bygone era - to call someone a hacker is to call them a true old-school master, an IT professional before there was any such thing as an IT professional. It simply doesn't make sense to refer to anyone as a hacker if they can't remember a time before desktop computers. There is no Internet-era equivalent of "hacker" - or if there is, I can't think of it. The PC Revolution is over, the dot-com bubble has burst. Technology is no longer the final frontier.

All your ideas of who I am are wrong. But I don't suspect you'll care enough to challenge yourself.

I don't wear a white, black, or gray hat. I don't type my sentences using numbers and punctuation marks instead of letters. I won't "teach you to hack," I don't "hack into computers," my goal is not to "hack the planet."

I am many things in many ways. I am young and old; I am male and female; I am Christian, Taoist, and Atheist. I am Black, White, and every color in between. I am college educated and a high school dropout. I work in a large corporation, part-time at the mall, and am unemployed. I am everything you can think of, but nothing you can understand.

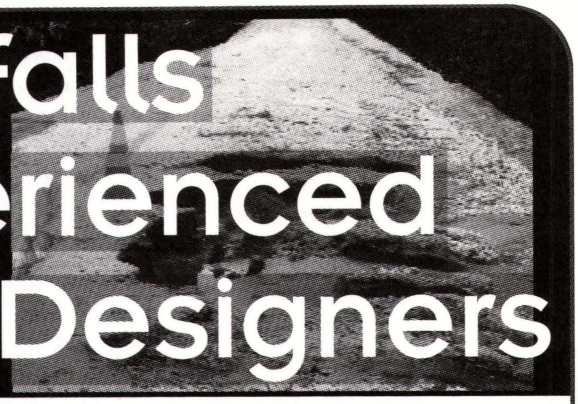
I do what I do because I love computers. I believe that information is amoral on its own, and that what I do with it is my own decision. "What I do" is whatever I find interesting at the moment; I don't worry about right or wrong, profit or loss, reputation or credibility. There have been countless nights that I have stayed up past 3:00 am working on something that has no inherent value other than the knowledge I gain from doing it. What I do goes beyond interest, beyond hobby, beyond obsession. Can you say the same about anything, *anything* that you do? If you can't, then you have gone through your life missing something.

I don't care what you think of me or what I do. I don't care what I think of you or what you do. I am not a zealot, bent on converting the world to my way of thinking - if I do something that interests you, I am happy to tell you about it if you ask. If you do something that interests me, I will ask you about it. My goal is to learn, which I will do with you but I can do just as well without you.

Call me a selfish bastard; call me a philosopher; call me a dreamer, an idealist; call me a criminal; call me a geek. Call me whatever you like.

Just don't call me a hacker.

Security Pitfalls for Inexperienced Web Designers



by Savage Monkey

I am a college student and I often have the opportunity to use and assist with websites developed by other students. Doing so has given me an appreciation for common security holes introduced by inexperienced web designers. Here I will provide a few examples of what not to do, or, from the sysadmin's point of view, what to make sure your users don't do.

First of all, validate *all* input, including get/post data you think only your own pages will produce, cookies produced by your own site, and, of course, user form data. Pay particular attention to anything where a parameter specifies a file to fetch or a command to run. One site I saw recently allowed users to specify, in a text field, arguments to fortune(6). The CGI script would then run something like "fortune $user ➥args" without any checks, allowing the user to pass a parameter like "; rm -rf" or literally anything else he wanted. If you really must put user data in backticks, consider giving the user a set of options to choose from. For instance, allow the user to check if he wants an offensive fortune, rather than letting him type any parameter he can think of.

Similar problems can occur when parameters specify files to fetch, especially with functions like "file" and "readfile" in PHP, which will work on virtually any resource, including local files and URLs. Many sites load different pages using something like "http://www.site.com/index.php ➥?page2fetch=sales.html". Lazy webmasters will neglect to verify that sales.html is indeed a part of the website, letting a malicious user specify page2fetch=/etc/passwd, for instance, to examine an arbitrary local file, or page2fetch=http:// ➥www.google.com, e.g., to use your site as a proxy. Some webmasters think they can solve this problem by appending a particular extension (html, say) to the page2fetch parameter. They're generally wrong. Enemies can circumvent this by appending a null character to the end of the parameter, tricking the system into ignoring the appended extension, and if this fails to work, they can still access unintended resources ending in the given extension. The only safe way to use this technique is to give index.php a whitelist of acceptable pages to fetch, and serving an error page if page2fetch is not on this list.

Use a similar method for other input as well. If your site requires someone to register with an email address ending in 2600.com, you may realize (as many webmasters fail to) that a malicious user could register with something like joe ➥schmo@gmail.com,nobody@2600.com -which, with poor authentication, would cause the registration info to be emailed both to joe ➥schmo@gmail.com and nobody@2600.com - or with something like <joeschmo@gmail.com>no ➥body@2600.com - where the email would be sent to joeschmo, with nobody@2600.com treated by the email system as a comment. Are there other tricks someone could use? Don't spend time sifting through the email RFCs trying to figure it out. Err on the side of caution, and make sure every email address matches some regexp like [A-Za-z0-9]+@2600\.com. If there's a problem, you'll hear about it. If an unauthorized user opens an account, you may not until after he's stolen confidential information, or whatever it is that you feel you need to protect. Use this technique everywhere. Don't try to look for weird patterns and rule them out; look for normal ones and allow them exclusively.

In general, don't believe anything your users tell you. If you're selling something, don't pass the price in URL or the postdata; just pass the item ID and look up the price in your own database. Use session keys; don't have the user pass the same authentication over and over where it's vulnerable to replay attacks. Don't assume that nobody will tamper with the postdata, or nobody will edit their cookies. Somebody will, and even if somebody doesn't, somebody else will read your code and laugh at you.

Also, don't reinvent the wheel, unless you're either really good or you just don't care. Don't invent your own new kind of encryption that looks pretty good to you. Don't even implement something you read about in cryptography class yourself. Why bother? People more paranoid than you or me devote their lives to doing it securely. Why not use their work?

Don't write your own forum software; download an open source package. They'll have more features than you have time to implement, a prettier look than you would have the patience to perfect and they'll have more eyeballs examining the code for bugs than you could ever have. Just make sure to keep the software up to date. A widely-deployed package with a well-known security hole is extremely dangerous, since script kiddies and worms will find you on Google and pick on you.

HTML, Perl, and PHP are easy. Downloading phpBB2 tarballs from the Internet and typing tar -xfz is even easier. Keeping your websites secure takes practice, but it's not impossible. Web design is one of the few fields in which it's possible to achieve greater security without compromising convenience and usability, so there's no reason to leave yourself (and your web host) vulnerable to attack.

A Peek Inside a Simple ATM Machine

by FocusHacks

In 21:4, I discussed the workings and "unofficial" reset method for LaGard ComboGard vault locks. This time I've got a whole ATM to work with.

The ATM I scored is a Diebold CashSource+ 100. This is one of those smaller indoor ATMs that you would find inside a convenience store. It features a monochrome LCD, eight option keys beside the screen, a number pad with four function keys (Shift, Cancel, Clear, and Enter), receipt printer, slots for one cash box and one "reject" box. The card slot is a horizontal swipe-through under the screen. There's a single five-tumbler lock on the front door. Once opened, you're given access to three things: The combination dial, the vault door bolt control, and a pair of buttons that lets you swing the top compartment upwards.

Once you squeeze the buttons together and swing the top compartment open, you're given access to the printer, the main power switch, the modem, and some Macintosh-style serial cables plugged into the backside of the LCD/keypad. The printer uses standard thermal receipt paper and there's only one printer, so there's no "live" paper audit trail. I'd imagine it's stored in memory, but it may not keep an audit trail at all. The modem in my ATM is a generic 33.6k serial modem. When I power the unit on, it attempts to dial the mother ship, but I am not curious enough to hook it up to a phone line to see what happens.

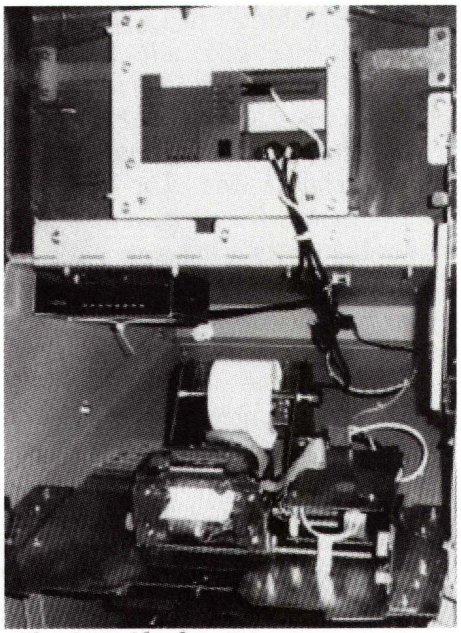


Fig. 1: Inside the upper compartment

Of course, all the interesting stuff is held within the vault. On my CSP-100, the vault lock was a LaGard 3332-3, which is a three number (0-100) mechanical combination lock with wires that can be used for sensing bolt position and a "duress" combination. These wires on my ATM were simply wire tied and unused. A duress combination is the combination you dial in when you're being forced against your will to open the

vault. To activate duress mode, you dial in the combination normally - except for the last digit which you dial to the "change" index, which is another mark about 20 degrees to the left of the "open" index. This causes a plastic arm inside the lock to trigger the duress switch.

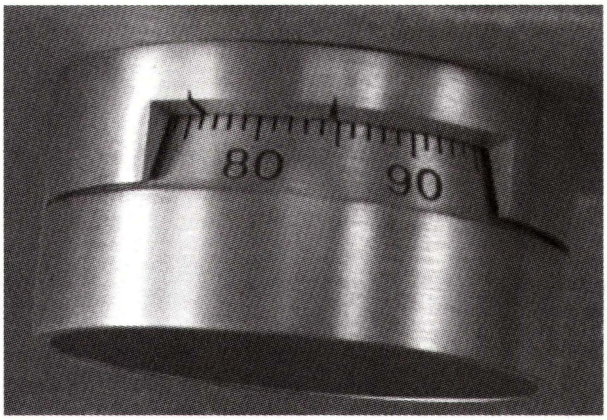


Fig. 2: Close-up of change index and open index marks

The duress wiring (white and blue wires) can be used in combination with a silent alarm or telephone dialer to notify the police or an alarm monitoring company. The bolt position switch that I mentioned (red and black wires) operates in the same way, but is triggered whenever the lock is opened regardless of duress mode. This can also be used with an alarm system or with a buzzer so that an audible alert is heard when the vault is opened.

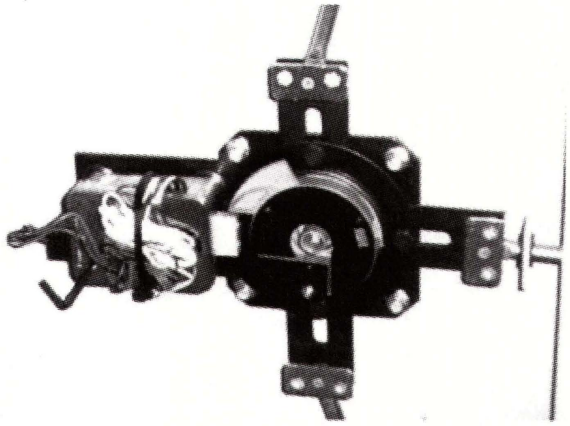


Fig. 3: Lock case w/ change key, alarm wiring & boltwork

This lock can be easily replaced with one of many combination locks on the market, including electronic combination locks such as the LaGard ComboGard I wrote about in 21:4, Kaba Mas (or Mas Hamilton) Cencon S2000, or Auditcon. The combination on the existing mechanical lock can also be changed provided you have a change key, which my ATM came with, taped to the vault door. Detailed combination changing instructions are available from LaGard. I found them by Googling for: change combination instructions group 2m.

Once the correct combination (or the duress combination) has been entered, the other knob will turn which retracts the locking bolts that hold the door shut. Once that knob is turned, the door opens and you've got full access to the cash boxes, reject box, the main power supply, control board, combination lock housing (for changing the combination using a change key), and the conveyor belt that moves the money around. The reject bin is where money goes that comes out of the cash box "out of spec," that is, multiple bills stuck together, bills that come out at an angle, folded, or damaged. There are several kinds of cash boxes. The one that came with my CSP-100 was a locking cash box that had a red/green tamper indicator on it. The locks on my reject box and cash box were both operated by the same 7-pin cylinder key. The tamper indicators will trigger at almost any sign of forced entry including simply removing them from the ATM. The boxes cannot be reinserted when the indicator is red, and the key is needed in order to clear the indicator.

The ATM knows what kind of cash boxes are inserted by means of an array of buttons inside the ATM that are operated by plastic nubs on the back of the cash box. I do not know what the coding is, but the reject box had its plastic nubs in a different pattern than the $20 cash box that my ATM came with. Most cash boxes can hold upwards of 2,000 bills (2,500 if they're fresh, crisp, new bills), so a fully loaded cassette of $20 bills could store up to $50,000. It's doubtful that you would see an ATM of this puny stature loaded with more than a few thousand dollars at any given time, though.

Pressing the small blue button on the lower front of the inside frame of the ATM allows you to firmly yank the innards out on a rolling rail system. This gives you better access to the money conveyor belt system, the main system board, the sides of the cash box area, and the main power supply.

Fig. 4: Rails extended, electronics and cash handler visible

The vault is made of heavy gauge steel, which probably is the main reason that this thing is so heavy. I certainly see why not very many ATM's get stolen. They might look small and easy to manage, but you would need two or three men and a pickup truck to make a successful and timely getaway with this small ATM, and good luck getting the vault opened up. It would certainly be more trouble than it's worth.I have not even tried to get into the ATM's diagnostics or settings yet. There are no power outlets in the storage unit I'm keeping the ATM in, so I'll have to move it somewhere else to continue tinkering beyond the mechanical realm. Given the severe lack of external controls (and a user or installer manual), I am thinking that the setup/maintenance process needs to happen either over the onboard modem, or with an external device such as the ATM programmers I've found in the dumpster before. I can't see where I'd hook such a device up though.

That's the mechanical breakdown of a simple ATM. As I experiment some more, look for another article on programming, setup, auditing, and diagnostics.

How to Get Responses Through Deception

by JFast

The other day I read an article that explained how to write emails that get responses. It said the usual things like make the subject line relevant, make your message clear, ask for an action statement, etc. *Boring!* I have found precisely the opposite: If you want to get responses to your emails, deceive people by making your email perplexing. The best way to do this is to write an imaginative email about something that could have happened but did not happen. You talk about phantom conversations, events, and meetings. Add plenty of details. The person reads your email and has no idea what you're talking about. What do they do? They respond. They simply can't ignore your email. You're capturing their interest and tricking them into responding to your gibberish.

For example, a friend had been ignoring my emails for weeks. So one day I wrote him a quick note about a phantom conversation we had on messenger. I added lots of details and ended my message with: "I enjoyed our chat the other day. I told you that idea totally sucked. Next time I will try not to dominate the conversation as much." On that same day I received his response:

"What the heck are you talking about? We didn't have a chat on messenger last night. What are you smoking brother? I haven't been going on my computer lately because of all the time I'm spending on it at work."

A few weeks back I met a friend by chance in the city library. I sent him an email describing another meeting we had at a different library branch. "I can't believe I saw you at the Marpole branch!" I wrote. His response:

"hahaha - well DON'T believe it! I didn't go near Marpole today! I worked at Fraserview actually. Wonder who you did see? If I have a twin I hope he doesn't make a habit of spending time in places I frequent...."

Another friend told me about an online game called Wordox and suggested we play each other one day. About a week later I sent her a message describing a game we supposedly played. "I enjoyed our wordox game the other day. I still think I could have beaten you...." She sent me a polite response:

"Glad you enjoyed the game, but unfortunately I don't recall playing against you. I usually play under Jade365 at home and at work under Cinynot. We should make arrangements to play sometime though."

For a lark I sent my sister a convoluted email about some cards she (supposedly) designed for me. Her response was quick and to the point:

"i have no idea what you are talking about!!!"

The next day I sent her a longer message:

"You and Leigh sent me a package from Kingston. In it Leigh has written a letter and you sent a post card from New York. Also, you put some cards that you designed inside the package. They were the ones that I sent you in the summer. DON'T YOU REMEMBER? You must have just sent this a few days ago, cause I just got it on Friday."

She was more confused than ever.

"I sent you a card from New York that is all I remember! Are you being facetious? I never designed anything and put it in a package. This is driving me nuts!!!!!!!!!!!!!!!!!!!!"

The trick is to make your email plausible. You need to mix things that did happen with things that did not happen. In the above example, my

sister is a designer, she did go to New York with Leigh, and she did send a card. The part about cards from the summer is pure fiction, designed to confuse her.

I felt guilty about an email I sent to a coworker of mine. I had been meaning to lend her a book about investing but I kept forgetting. So I sent her an email implying that I gave her the book. She wrote back:

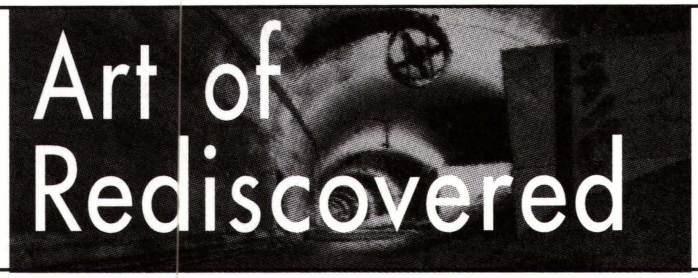
"Hi. I don't have the book!!! Where is it? Did you leave it at work for me? Thank you very much if you did, however, I didn't get it. I will be there Thursday night, at the game so I will pick it up then. Thank you again..."

Oops. Poor girl is expecting to receive the book on Thursday! I sent her another email describing when and where I gave it to her - all lies of course. She wrote back:

"You must have me confused with the other Karen that works in the same office and likes to run marathons and trade stock in her spare time. Because this Karen did not get any photocopy of a book. I haven't been at briefing since I don't know when, as I always work during the week starting @ 5pm, just after the briefing. Are you giving me the goat??????"

I've found that this technique works wonders, especially the first few times you use it. It goes without saying that if you do this too much, people will become wise to your tricks and will once again ignore you. The lesson here is that people don't have a problem ignoring a real email. But as soon as you write an email that makes you look like you've made a mistake or mixed something up, they will respond immediately to correct you. Use this piece of human psychology to your advantage!

The Ancient Art of Tunneling, Rediscovered



by Daniel
daniels@stud.cs.uit.no

This article will teach you how to use pay-per-use wireless networks for free. It works on many (but not all) networks (wireless or not), and is based on a very simple principle: Tunneling. I'm sure we have all seen how useful tunnels can be, be it for making our communications secure over an ssh tunnel or to spoof your IP. This article will show you how to tunnel TCP connections over ICMP packets.

Why Tunnel Over ICMP?

I have been traveling a lot over the past year. During that time, I've come across many wireless networks, aimed specifically at Internet-hungry travelers dying to check their mail. Of course, most of these networks will redirect you to a "we accept the following credit cards" page whenever you try to surf the web, and simply drop any other traffic (such as that on port 22).

Remarkably however, it turns out that many of these wireless networks allow you to ping remote hosts. This makes tunneling over ICMP a very attractive prospect, especially as they don't impose any particular size or content limitations on the ping packets. After a search of the net for a tool to do the job turned up nothing, I decided to write my own, called ptunnel (see below for a URL). The remaining part of this article will explain how ptunnel works, how you can set it up yourself, some situations where it might be useful, and finally some performance numbers.

The Basics of ICMP Messages

ICMP stands for Internet Control Message Protocol. It has many different message types, but the most well known are probably echo request/reply (ping) and time-to-live exceeded error messages (traceroute). We will build our tunnel using the echo request and reply packets, which look like this:

```
[  IP header (20 bytes)  ]
[ Type | Code | Checksum ]
[ Identifier  | Seq. no  ]
[ Data..arbitrary length ]
```

Type and code are 8-bit values, with type 0 indicating an echo reply, and type 8 indicating an echo request. The checksum, identifier, and seq.no fields are 16-bit values. The checksum is the usual IP checksum, calculated over the entire ICMP packet starting with the type field, with the checksum field set to zero for the calculation. For more details, see RFC 792 (ICMP). The nice thing about these packets is that they allow an arbitrarily long data chunk at the end, which makes them well suited for carrying our tunnel data.

Tunneling

Tunneling naturally requires two parties, a proxy and a client. The proxy will be responsible

for relaying the packets it receives over TCP to the host we wish to connect to, and the client will be our computer, accessing the net from some public wlan. We will use the identifier field of the ICMP packet to identify different tunnel sessions. The tunnel setup looks something like this:

```
App <-- TCP --> [client]
                    |
               ICMP tunnel
                    |
              [proxy] <-- TCP -->
➥Destination server
```

The client receives incoming connections from clients (that would be your ssh client, for instance), and sets up a bi-directional tunnel with the proxy, using ICMP packets. The proxy deals with connecting to the destination server (for instance, your ssh login server) using a normal TCP connection. The ICMP message exchange basically goes like this:

1. The client sends an echo request packet with some data to the proxy.

2. The proxy responds with an echo reply packet.

The proxy's reply will be in addition to the automatically generated OS response (which contains the data we just sent to the proxy). Every packet includes a sequence number (different from the one in the ICMP header), an acknowledgment number, message type, and the destination's IP address and port. The message type simply specifies what kind of message we're dealing with: new tunnel request, data, acknowledgment, or close. Most messages fall in the data and ack categories.

Whenever the proxy receives data from the destination server, it is sent to the client as echo reply messages. We can't use echo request packets here, as they may not make it past the (possibly) NAT'ed network on the other end, causing our tunnel to break down. Similarly, the client will forward data from the connecting application using echo request packets.

Reliable Tunneling

In order to tunnel TCP over ICMP, we will need to re-implement TCP's reliability and message ordering, as ping packets have a nasty tendency to get lost or swapped along their way. For reliability, the two peers maintain a record of the last packet acknowledged by the remote end, and will initiate packet resends of the first non-acked packet after some delay. The sequence numbers ensure that we maintain TCP's ordered message delivery. Finally, send and receive windows prevent the two peers from having too many non-acked packets in-flight, much in the way TCP uses a window size to constrain the amount of outstanding, non-acked data, although the window size used in ptunnel is static.

Surfing For Free

To use ptunnel, you need to have a computer somewhere that is pingable from the rest of the Internet. You'll also need root access on that computer, and it should run some flavor of Linux, Un*x, or BSD. A similar setup is required for the client, although our only requirement for the network is that we can ping hosts outside the network (this can be easily verified by pinging your proxy host). All other protocols can be blocked.

Before using ptunnel to surf from the client computer, you'll need to start ptunnel up on your proxy computer:

```
[root@proxy]# ./ptunnel [-c <device>]
```

The -c argument is optional and specifies whether (and on which device) packet capturing is to be used. You should test without it in a controlled environment first, as using packet capturing on the proxy tends to diminish bandwidth quite a lot. I know Mac OS X requires it either way, but YMMV.

Next, on your client computer, start ping tunnel as follows:

```
[root@client]# ./ptunnel -p <proxy's IP
➥addr> -lp 8000 -da somehost.somewhere
➥.com -dp 22 [-c <device>]
```

Again, the -c argument is optional. Here we specify where our proxy runs (this is the host we will be pinging) using the -p switch and a local listening port using -lp. Applications can now connect to your client computer on that port and get their connections tunneled over ICMP.

The -da and -dp switches specify the destination address and port. In this case I've specified port 22, as I want to tunnel an ssh connection over ICMP. To use the tunnel, I would simply do the following:

```
[user@client] ssh -l user -p 8000 local
➥host
user@localhost's password:
```

Note that tunneling ssh makes the tunnel very versatile, as you can then tunnel additional TCP connections over TCP, adding encryption to the existing ICMP tunnel. This can be very useful when you're surfing in such a (presumably) hostile environment as this.

Where To Use It

In general, ping tunnel is only useful if you find yourself in a situation where you need to access the net but your only network access is blocked by port, protocol, or content filters. Your employer may be monitoring/blocking TCP traffic but not ICMP packets. Many wireless network providers charge a fee for using their networks but fail to block outgoing and incoming ICMP packets. This is another area of potential use for

ptunnel. I can't speak for the U.S., but in Europe many wlans fit the above description, including airport wlans in Norway and Germany. I have tested ptunnel on some of these networks and it does indeed fulfill its promises.

Keep in mind though that you are *not* surfing anonymously here - all your connections will appear to come from the proxy computer. It would also be trivial to detect the IP address of the proxy computer for the person(s) running the network your client is running on, as there would be a lot of "strange" ICMP traffic to and from that IP.

Performance

Ptunnel performs well enough for my needs. In my testing, it has reached speeds of 150 kb/s down and about 50 kb/s up. This can be further improved upon by tuning various parts of the code (the ack intervals and window sizes are the most obvious candidates here, but gains may also be possible by tweaking the max size of the ping packets sent), but that is left as an exercise for the reader. The source code is available and freely distributable (see references).

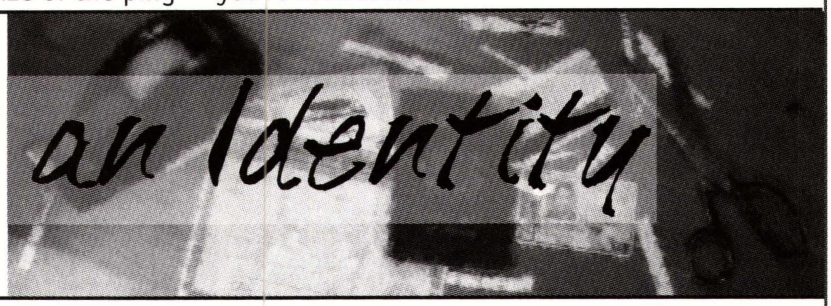
And finally: It *can* fail.

Ptunnel isn't perfect and there are some problems that it can't get around. If you can't ping your proxy computer then you're out of luck. If the service provider you're using is doing some sort of filtering of incoming echo replies, you may also find yourself out of luck. Finally, I won't say anything as to the legality of this technique, so use it at your own risk. Keep in mind that tracing you to the proxy you are using is trivial.

References

For more info on ICMP, check out RFC 792. Ptunnel's source code can be downloaded from this URL: <http://www.cs.uit.no/~daniels/➥PingTunnel/>. There are also some more in-depth technical details explained there if you're interested.

Forging an Identity



by SistemRoot

Many hackers don't limit themselves to the world of computers and networks but explore weaknesses in all systems.

I was intrigued with obtaining false identification so I set out to figure out a way it could be done. But how can you possibly duplicate an identification card with all the ways they try to prevent this from being done such as holograms? Well... you don't. With all the protection they have to keep anyone from reproducing an ID, the two documents you need to obtain an *actual* ID are easily forged, making all those anti-counterfeiting methods useless.

First, the birth certificate. Depending on the year and location of birth, the paper and style of the certificate varies. The one I worked with is nothing more than a photocopy on regular paper with a raised seal. Using "The Gimp" or "Photoshop" and a typewriter, it can easily be reproduced. The same thing applies with the Social Security card. It takes some time tweaking the color to get it right. The paper is simply non-glossy card stock. With a paper-cutting tool found at office supply stores, a perforated edge can be created. However, getting a raised seal on a birth certificate takes some social engineering, a small manufacturing company of paper embossers, and a Trac phone. If you want a real registered copy, it is easy to get with the right information.

With these two documents anyone can get a photo ID. Standard state photo IDs are offered at License Bureaus and once someone has obtained a false photo ID, it isn't hard to gain other forms of ID to back it up. But of course this is just an ID and unless they have used an actual Social Security Number and real information on the birth certificate, it won't pass when opening bank accounts and signing up for certain jobs. For someone to do this, they would need to find information on a person who was born around the same time as they were and died under the age of six months or passed away in a different state from their birthplace. Because of this, there wouldn't be any state or work records of them being deceased. This information can be found at the library's newspaper archives under the obituary section. Pretending to be this person, they could write the county courthouse and request and obtain an actual registered copy of the birth certificate. Getting an actual Social Security Number isn't hard ether. Anyone can apply for a Social Security Number over the phone and getting a Social Security card can be done by mail.

Now the person would have a new identity and the means for getting a driver's license, passport, state ID, bank accounts, credit cards, or basically anything.

Marketplace

Happenings

INTERZONE GOES WEST! While the Atlanta Interz0ne stays hacker con, Interz0neWest will be a more professional style I.T. conference, carrying on in the tradition of "effecting change through education." Along with Interz0neWest, GRAYAREA - the non- traditional security academy - will be happening, teaching methodologies and skills instead of test answers! San Francisco Bay Area in early October 2005. See interz0ne.com or grayarea.info for the latest details.

PHREAKNIC 9: THE REVOLUTION WILL NOT BE TELEVISED. Join the longest running technology and culture convention in the Southeast for our ninth year of communication, conflagration, madness, moxie, and general mayhem. We'll have technical presentations, sci-fi and tech culture exhibits and panels, and the usual round of paranoid ramblings and conspiracy theories. Come learn, teach, and make merry with us - before the Ministry of Truth can tell you not to! October 21-23, 2005. More info at http://www.phreaknic.info.

For Sale

CUSTOM T-SHIRTS: Why be EXACTLY like everyone else? Let's face it, we're all individuals and there's a little revolutionary in each of us. It's high time that you nurture this, and a hand silk screened shirt featuring you as Che Guevara is the perfect way to start. Available on a wide variety of quality shirts with a wide selection of ink colors. And for those who are living life on the cheap, we also offer heat transfer shirts in a limited number of colors. Visit http://meguevara.com. OVERSTOCK: We found a limited number of "Hello My Name Is _____ and I'm a Hacker" shirts left over from Beyond HOPE in 1997. Each shirt ships with a Sharpie so you can add your own name, handle, moniker, nom de plum or paw print. See our specials section for more details.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for *2600* subscribers: Mention *2600* and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you deserve.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

PHRAINE. The technology without the noise quarterly would like to thank the *2600* readers who have also become new subscribers and encourages those who have not ACK their need for diverse computer information in conjunction with that of *2600* to dedicate some packets and become a subscriber today! Visit us at our new domain www.pearlyfreepress.com/phraine.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your *2600* reader price discount.

FILE TRACKING SOFTWARE: File Accountant(TM). Windows XP and later. Creates a list of files on your hard drive. Run it before and after installing new products and/or updates to discover which files are added/changed/deleted. Print lists. Other features. More information at: http://abilitybusinesscomputerservices.com/fa.html or fa.info@abilitybusinesscomputerservices.com.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

CABLE TV DESCRAMBLERS. New. $75 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tac-

tics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. Graduate of Yale College and Stanford Law School. Years of experience defending human beings facing computer-related charges (also specializing in cannabis cultivation and medical marijuana cases). Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

FAST CASH OK! 100% online Instant Approval. NO CREDIT CHECKS. Up to $500 in your bank tomorrow! www.FastCashOK.com "Hacker owned and operated"

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or exploit? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over nine years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. Our office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2004 are now available in DVD-R format for $30! Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

I-HACKED.COM. Taking advantage of technology by hacking today's electronics and systems to better our lives. Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

OFFLINE OUTLAW IN TEXAS needs help! I've gone 8 years but may go home in 2010 and want to start getting back up to speed. Our library leaves much to be desired in the areas I'm looking. If you have a curious, creative mind and are patient enough to answer my questions and help me learn, please drop me a line. I'll answer all letters. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

ICEDRAGON FOUNDER OF XPH. I am mostly interested in finding people and fellow hackers that remember me and my crew from Dalnet (irc.dal.net). If you were a part of XPH on Dalnet or just someone who used to stop by, please write me. I have been in prison for the past two and a half years and have lost contact with mostly everyone. I still have seven and a half years to go and would like to locate and talk with all my old friends, especially ^chmod, DjFlipper, KORNOGRAPHY, Chuco, Hackerish, ccarderz, MastarP, xXCrackXx, Flair, PacMan, Bratty, Miss Angel, and of course everyone I didn't have room to mention! Also, any other hackers or phreakers that would like to write me, please do. I will respond to ALL letters, hackers or not. Brandon Kaufman, #15111040, 82911 Beach Access Rd., Umatilla, OR 97882.

STILL IN THE BIG HOUSE. Over three down, about a year left to serve. Known as Alphabits, busted for hacking some banks and doing wire transfers. I'm bored to death and in desperate need for stimulation. I would love to hear from ANYONE in the real world. Help me out and put pen to paper now. Why wait? Will reply to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 190 lbs., 25 years old (for the ladies - please send photos, will do same), been in 6 years with a couple to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, vaults, locks, alarms, and anything novice-level from *2600.* Need placement on various mailing lists: video, DVD, book, magazine, and ANYTHING you can think of is appreciated. Anyone know of hacker mag besides *2600?* Mycology, anyone? Let's talk! I love photos! Send mail to: Henry French #44552-083, PO Box 10 (Elkton FCI), Lisbon, OH 44432.

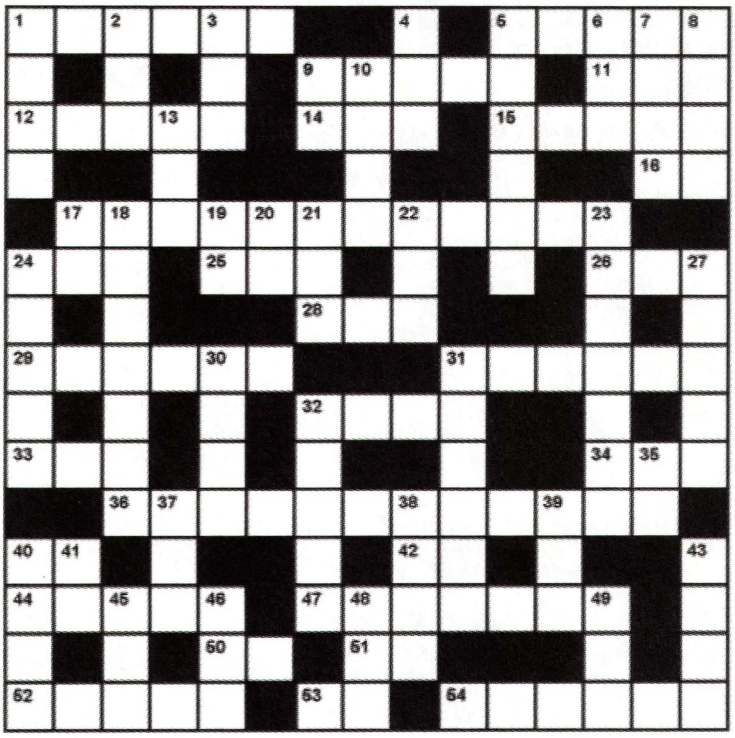
CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953.
Deadline for Winter issue: 11/15/05.

謎謎

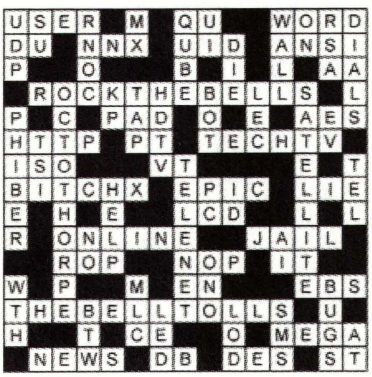


Across

1. Speakers' _____
5. (9-Across company)
9. _____ Card
11. Mr. Anderson
12. DJ Slider
14. prot. (w/ 49-Across)
15. Method of destruction
16. Estonia
17. Reach out and _____
24. Your number here (abbr.)
25. Batt. backup
26. _____ partner
28. MIN's partner
29. Network type
31. First toy phone
32. Cipher
33. "You will" company
34. Blogger's feed
36. Sprint let you do this
40. AM's partner
42. Old Mac
44. Hackers At _____
47. Kevin's foil
50. Hack-Tic home
51. (See 14-Across)
52. Speakers' _____
53. AOL trademark
54. DVD replacement

Down

1. Internet location
2. Brazilian net
3. Bug
4. Fetch, et al.
5. Once a hacker's telco target
6. Nortel's development arm
7. Std. org
8. Program
9. Attach a dsk (Unix)
10. Repeat
13. School addr.
17. State of Gore
18. Spa for a droid
19. SYS. V dialer
20. Former Compaq rival
21. American identity
22. Device for 9-Across
23. _____ mechanical
24. 64-bit processor
27. Data place before bases
30. Not DES
31. Port 23
32. _____ Access Terminal
35. VHS speed
37. _____ head
38. Your time _____
39. DIMM, SIMM, et al.
40. Bug
41. _____ Bell
43. Group of peers
45. Zip alternative
46. Last statement
48. GSM chip
49. Modem co. or directory



http://www.2600.com/puzzle

FOOL

HIDDENMESSAGEHIDDENMESSAGEHIDDENMESSAGETHISISNOTAHIDDENMESSAGE

That's what you should be calling yourself if you didn't enter the *Freedom Downtime* Easter Egg Hunt. If you had, you would be enjoying the following right now:

- Lifetime subscription to *2600*
- All back issues
- One item of every piece of clothing we sell
- An *Off The Hook* DVD with more possible Easter Eggs
- Another *Freedom Downtime* DVD since you will have probably worn out your old one
- Two tickets to the next HOPE conference

But you didn't enter, did you? We know you didn't because we didn't receive ONE SINGLE ENTRY from any of you lazy readers. Not one! Hard to believe but true.

Yes, it's a difficult contest. It's supposed to be. But the best entry is the one that wins even if it only gets one answer correct. In this case, ANY entry would have won by default.

Submit entries to:
Easter Egg Hunt c/o 2600, PO Box 752, Middle Island, NY 11953 USA
You can get the *Freedom Downtime* double DVD set by sending $30 to the above address or through our Internet store located at store.2600.com.

So let's try this one more time. We're looking for the best list of Easter Eggs on our *Freedom Downtime* documentary. What constitutes an Easter Egg? Anything on the DVDs that is deliberately hidden in some way so that you get a little thrill when you discover it. When you find one of these, we expect you to tell us how you found it and what others must do to see it. Simply dumping the data on the DVD won't be enough to yield this information.

It's possible that there are some Easter Eggs that don't require you to hit buttons but that contain a hidden message nonetheless. For instance, if you discover that taking the first letter of every word that Kevin Mitnick says in the film spells out a secret message, by all means include that. We will be judging entries on thoroughness and there is no penalty for seeing an Easter Egg that isn't there. You can enter as many times as you wish. Your best score is the one that will count. Remember, there is no second place! The new deadline is November 15, 2005 and this is the only time we'll be extending it. All entries must be sent through the regular mail and not over the Internet.

Do you find it annoying that you had to leave your house to find a copy of 2600?

Did you know there is an easy solution that involves not having to leave your domicile at all?

It's called the 2600 Subscription and it can be yours in a couple of ways. Either send us $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA. Or subscribe directly from us online using your credit card at store.2600.com. Then just sit back and wait for issues to come hurtling to your door as if by magic.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

Vancouver: Pacific Centre Mall Food Court.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, Cottingham Road, opposite Hull University. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth St. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Morgan's Coffee & Tea, 498 Washington St.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Camille's at the corner of Sunrise and Madison.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Santa Barbara: Cafe Siena on State St.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Union Station in the Great Hall near the payphones. 5:30 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Corner Coffee, SW corner of 11th and Alabama.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Wilmington: Independence Mall food court.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Akron: Arabica on W. Market St., intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Blvd. entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.

Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 6 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

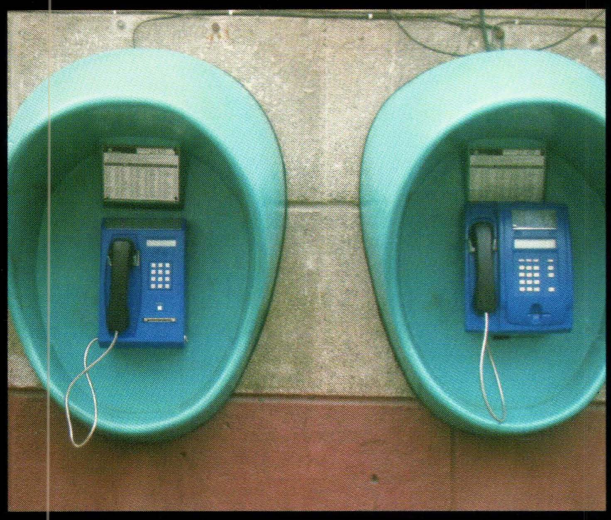
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones of the World

Belarus. A pack of payphones hangs out in the streets of Minsk.



Belarus. A closer look at two of them with subtle differences.

Russia. These were found in the city of Yekaterinburg.

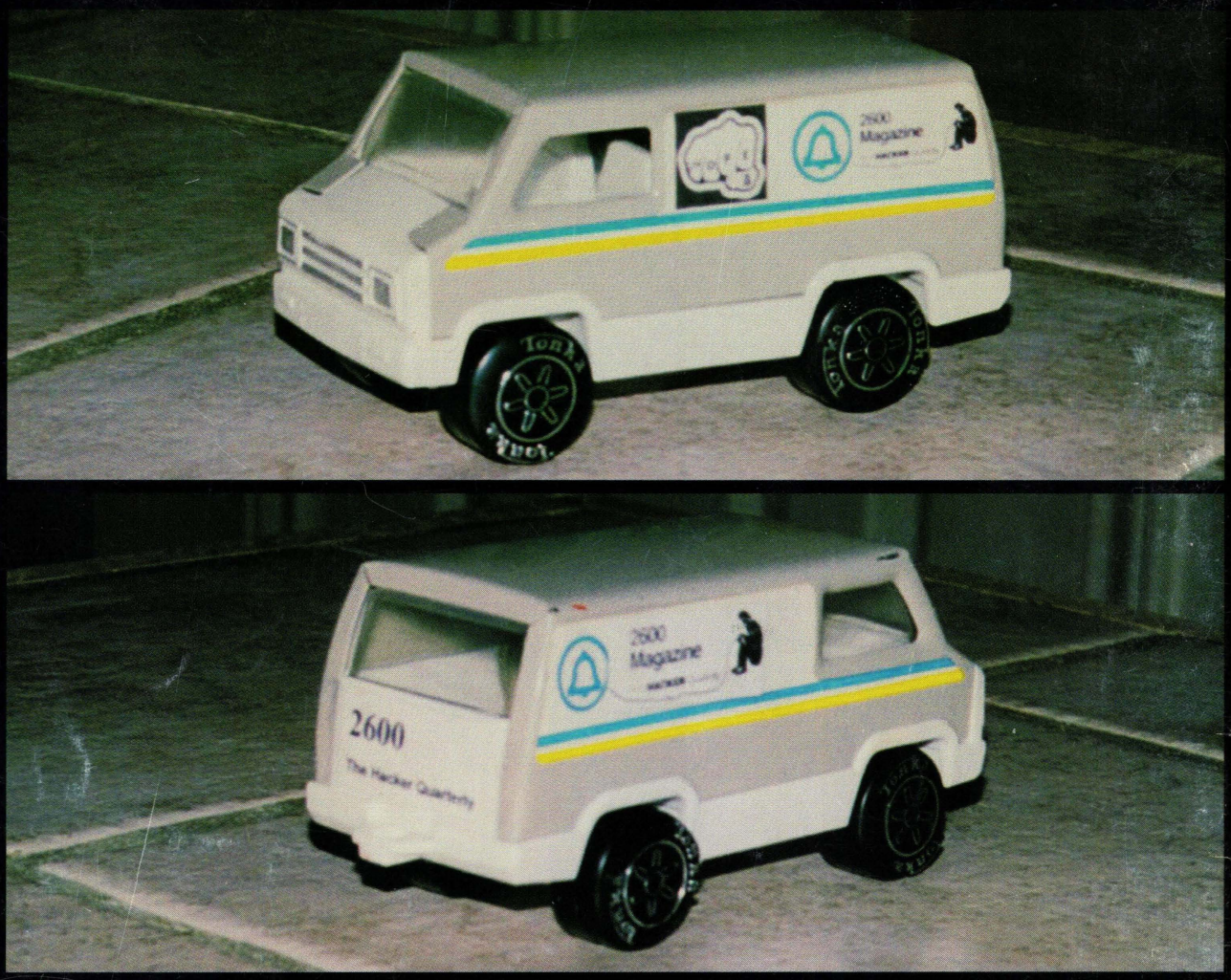
Russia. Very clean and rarely used due to the prevalence of mobile phones.

Photos by Emmanuel Goldstein

Payphones that used to be on the other side of this page can now be found on Page 2!

To see even more payphone photos online, visit http://www.2600.com/phones.

The Back Cover Photo



From the Some People Have Entirely Too Much Time On Their Hands Dept., here is a true "minivan" recreation of our own 2600 van, made from a Tonka toy phone van picked up at an antique shop in Austin, Texas. The tires are a little weird and our rear end looks a lot better, but it's a valiant effort.

Photos by Golden Helix

Do you have a photo for the back page?

Mail it on in to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 or email it to us at articles@2600.com. (Yes, we know it's not technically an article but please humor us.) When taking digital photos, be sure to use the highest possible resolution. If we use your picture, you'll get a free subscription (or back issues) and a 2600 t-shirt.